(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10022996 A**

(43) Date of publication of application: **23 . 01 . 98**

(51) Int. Cl **H04L 9/36**

(21) Application number: **08169950**

(22) Date of filing: **28 . 06 . 96**

(71) Applicant: **MITSUBISHI ELECTRIC CORP**

(72) Inventor: **FUNABE CHIEKO**
BABA YOSHIMASA
SENOO SHOICHIRO
ATSUI YUJI

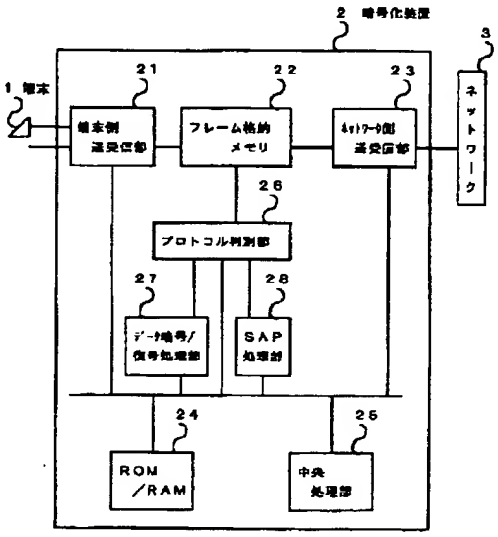
(54) **CIPHERING DEVICE**

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To realize password communication through the use of a network unit which does not have the function of ciphering by converting a service type into password communication so as to transmit to when the service type is non-password communication.

SOLUTION: A terminal-side transmission/reception part 21 stores a reception frame in a memory 22. A network-side transmission-reception part 23 stores the reception frame in the memory 22. A protocol discrimination part 26 discriminates the protocol of the frame, transmits it an the time of an RIP frame and transfers control to a SAM processing part 28 at the time of an SAP frame. When the processing part 28 receives the SAP frame from a terminal 1, it converts the non-password service of the service type into password service and transmits it to a network 3 through the transmission/reception part 23. When the SAP frame is received from the network 3, the password service of the service type is converted into the non-password service, the number of hops is set and it is transmitted to the terminal-side 1 through the transmission/reception part 21.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－22996

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ　9/36			Ｈ０４Ｌ　9/00	６８５	

審査請求　未請求　請求項の数３　ＯＬ　（全 22 頁）

(21)出願番号　特願平8－169950

(22)出願日　平成８年(1996)６月28日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　舟辺　千江子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　馬場　義昌
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　妹尾　尚一郎
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　弁理士　宮田　金雄　（外３名）

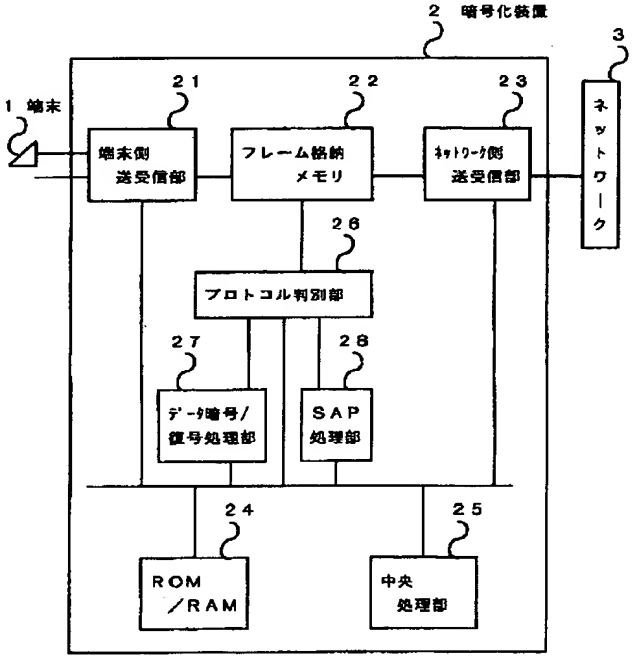
最終頁に続く

(54)【発明の名称】　暗号化装置

(57)【要約】

【課題】　既設のサーバ、クライアントまたはルータなどの暗号化機能を持たないネットワーク機器を用いて暗号通信ができる暗号化装置を提供する。

【解決手段】　端末とネットワーク間に暗号化装置を接続し、端末からのデータを暗号化してネットワークへ送出し、ネットワークからのデータを復号して端末へ送信し、端末とネットワーク間の接続制御フレームは暗号化しない。



1

【特許請求の範囲】

【請求項１】　クライアントの機能をもつ端末とサーバの機能をもつ端末とがネットワークを介して接続し、複数のネットワークが存在する場合にはネットワーク間をルータで接続するローカルネットワークで、暗号通信を行うために前記端末とネットワーク間に挿入接続する暗号化装置において、以下の構成要素を有することを特徴とする暗号化装置。

１．前記端末からサーバ情報を通知するフレームを受信し、このフレームのサーバ情報に含まれるサーバのサービスタイプが非暗号通信なら、そのサービスタイプを暗号通信に変換し、そのフレームを前記ネットワークに送信する暗号サービス化手段、

２．前記ネットワークからサーバ情報を通知するフレームを受信し、このフレームに含まれるサーバ情報のサービスタイプが、暗号通信なら非暗号通信に変換して前記端末に送出し、非暗号通信ならそのサーバ情報を廃棄するか、ルータを中継した数示すホップ数を到達不能の値に変換して、そのフレームを前記端末に送出する非暗号サービス化手段、

３．前記端末からデータフレームを受信し、このデータフレームに含まれる所定のデータ部を暗号化して前記ネットワークに送信する暗号化手段、

４．前記ネットワークからデータフレームを受信し、このデータフレームに含まれる所定のデータ部を復号して前記端末に送出する復号手段、

５．前記端末から通信経路情報を通知するフレームを受信し、このフレームを前記ネットワークに送出し、前記ネットワークから通信経路情報を通知するフレームを受信し、このフレームを前記端末に送出する通信経路情報中継手段。

【請求項２】　クライアントの機能をもつ端末とサーバの機能をもつ端末とがネットワークを介して接続し、複数のネットワークが存在する場合にはネットワーク間をルータで接続するローカルネットワークで、暗号通信を行うために前記端末とネットワーク間に挿入接続する暗号化装置において、以下の構成要素を有することを特徴とする暗号化装置。

１．暗号化除外対象のアドレスを記憶する透過処理アドレステーブル、

２．前記端末からデータフレームを受信し、このデータフレームの宛先アドレスが前記透過処理アドレステーブルに登録されているならデータフレームの所定のデータ部を暗号化せずに、登録されていないならデータフレームの前記所定のデータ部を暗号化して、前記ネットワークに送出する暗号化手段、

３．前記ネットワークからデータフレームを受信し、このデータフレームの送信元アドレスが前記透過処理アドレステーブルに登録されているならデータフレームの前記所定のデータ部を復号せず、登録されていないならデータフレームの前記所定のデータ部を復号して、前記端末に送出する復号手段、

２

４．暗号化対象外のサーバのサーバ情報を記憶する透過処理サーバテーブル、

５．前記ネットワークからサーバ情報を通知するフレームを受信し、このフレームのサーバ情報に含まれるサーバ名と前記透過処理サーバテーブルに記憶されているサーバ名との比較結果に基づいて前記フレームを前記端末に送出するサーバ情報通知フレーム透過処理手段、

６．前記端末から通信経路情報を通知するフレームを受信し、このフレームを前記ネットワークに送出し、前記ネットワークから通信経路情報を通知するフレームを受信し、そのフレームを前記端末に送出する通信経路情報中継手段。

【請求項３】　クライアントの機能をもつ端末とサーバの機能をもつ端末とがネットワークを介して接続し、複数のネットワークが存在する場合にはネットワーク間をルータで接続するローカルネットワークで、暗号通信を行うために前記端末とネットワーク間に挿入接続する暗号化装置において、以下の構成要素を有することを特徴とする暗号化装置。

１．前記端末からサーバ情報を通知するフレームを受信し、このフレームのサーバ情報に含まれるホップ数に所定の数を加えたフレームを前記ネットワークに送信するホップ数加算手段、

２．前記端末から、立ち上がり時の接続相手のサーバ情報を要求するフレームを受信し、所定の接続相手のサーバ情報を通知するフレームを前記端末に送出する立ち上げ要求応答手段、

３．前記ネットワークから、立ち上がり時の接続相手のサーバ情報を要求するフレームを受信し、廃棄する廃棄手段、

４．前記端末からのデータフレームを受信し、データフレームの所定のデータ部を暗号化し、前記ネットワークに送出する暗号化手段、

５．前記ネットワークからのデータフレームを受信し、データフレームの前記所定のデータ部を復号し前記端末に送出する復号手段、

６．前記端末から通信経路情報を通知するフレームを受信し、そのフレームを前記ネットワークに送出し、前記ネットワークから通信経路情報を通知するフレームを受信し、そのフレームを前記端末に送出する通信経路情報中継手段。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は複数のサーバとクライアントを暗号化装置を介してネットワークに接続し、データを暗号化して相互に通信を行う暗号化装置に関する。

【０００２】

【従来の技術】従来の暗号化装置は受信したフレームを全て暗号化して送信し、ネットワークシステムを運用するための制御フレームも暗号化されていた。そのため、暗号化機能を持たないネットワーク機器や端末とネットワークシステムを運用するための制御フレームを交換することができず、ネットワーク機器を介してフレームの中継を行う場合は、特開平4−154233号公開に示された暗号化装置のようにネットワーク機器も暗号化機能を備える必要があった。システム構成図を図２９に示す。図２９において、(1)は端末相互間の暗号系、(2)はネットワーク内の暗号系、NW11、NW12、NW13はネットワーク、21、22は通信バス、31、32、33はブリッジなどのネットワーク機器、111、112、121、122、131、132は端末である。

【０００３】次に動作について説明する。図３０はＩＰ（Internet Protocol）フレームを例とした暗号化範囲を示すフレーム図である。送信端末111は相手端末121との通信に必要な情報のみには、端末相互間の暗号系(1)を適用し、ネットワークNW11、NW12やネットワーク機器31、32での転送処理などに必要な情報には、ネットワーク内の暗号系(2)を適用する。即ち、送信端末111は、自分の属するネットワークNW11と相手端末121の属するネットワークNW12とを接続するネットワーク機器31、32のネットワークのアドレス等のネットワーク内のみで使用する情報には該ネットワーク内の暗号系(2)により図３０のN1、N2、N3部分を暗号化し、両端末(111、121)相互間のみの情報には該端末相互間の暗号系(1)で図３０のT1、T2、T3部分を暗号化し、一つのメッセージとして自分111の属するネットワークNW11へ送出する。

【０００４】そしてネットワークNW11に接続されたネットワーク機器31は該メッセージを受信し、該ネットワークNW11で使用する図３０のN1、N2、N3部分を解読し、相手端末121の属するネットワークNW12と接続されるネットワーク機器32へ転送する。ネットワーク機器32も、同様にネットワークNW12で使用する図３０のN1、N2、N3部分を解読し、該ネットワークへ該メッセージを送出する。ネットワークNW12に属する相手端末121は、ネットワーク機器32から受信したメッセージの中のネットワークで使用する図３０のN1、N2、N3部分をネットワーク内の暗号系(2)で解読し、自分宛であることを認識して端末間の情報である図３０のT1、T2、T3部分を、端末相互間の暗号系(1)で解読する。

【０００５】従来の暗号化装置においては、ネットワーク装置間の暗号系と端末相互間の暗号系とに分け、ネットワーク装置は中継に必要な部分を復号し、解読することにより、ネットワーク機器を含むネットワークを介して行う端末間のメッセージ通信を暗号化し、当該端末間では正常通信を行える通信秘匿方式を提供している。

【０００６】

【発明が解決しようとする課題】従来の暗号化装置は以上のように、ユーザのデータフレーム以外のネットワークシステムを運用するためのネットワークシステム制御フレームも暗号化していたため、暗号化機能を持たないネットワーク機器や端末とネットワークシステム制御フレームの交換ができなかった。本発明はかかる課題を解決するためになされたもので、既設のサーバ、クライアントまたはルータなどの暗号化の機能を持たないネットワーク機器を用いて暗号通信ができる暗号化装置を得ることを目的とする。

【０００７】また、暗号化装置が接続されたクライアントから暗号化装置の接続されていないサーバにアクセスできる暗号化装置を得ることを目的とする。

【０００８】

【課題を解決するための手段】第１の発明に係わる暗号化装置は、端末からサーバ情報を通知するフレームを受信し、このフレームのサーバ情報に含まれるサーバのサービスタイプが非暗号通信なら、そのサービスタイプを暗号通信に変換し、そのフレームをネットワークに送信する暗号サービス化手段と、ネットワークからサーバ情報を通知するフレームを受信し、このフレームに含まれるサーバ情報のサービスタイプが、暗号通信なら非暗号通信に変換して端末に送出し、非暗号通信ならそのサーバ情報を廃棄するか、ルータを中継した数を示すホップ数を到達不能の値に変換して、そのフレームを端末に送出する非暗号サービス化手段と、端末からデータフレームを受信し、このデータフレームに含まれる所定のデータ部を暗号化してネットワークに送信する暗号化手段と、ネットワークからデータフレームを受信し、このデータフレームに含まれる所定のデータ部を復号して端末に送出する復号手段と、端末から通信経路情報を通知するフレームを受信し、このフレームをネットワークに送出し、ネットワークから通信経路情報を通知するフレームを受信し、このフレームを端末に送出する通信経路情報中継手段とを有するものである。

【０００９】第２の発明に係わる暗号化装置は、暗号化除外対象のアドレスを記憶する透過処理アドレステーブルと、端末からデータフレームを受信し、このデータフレームの宛先サーバアドレスが透過処理アドレステーブルに登録されているならデータフレームの所定のデータ部を暗号化せずに、登録されていないならデータフレームの所定のデータ部を暗号化して、ネットワークに送出する暗号化手段と、ネットワークからデータフレームを受信し、このデータフレームの送信元アドレスが透過処理アドレステーブルに登録されているならデータフレームの所定のデータ部を復号せず、登録されていないならデータフレームの所定のデータ部を復号して、端末に送出する復号手段と、暗号化対象外のサーバのサーバ情報を記憶する透過処理サーバテーブルと、ネットワークからサーバ情報を通知するフレームを受信し、このフレームのサーバ情報に含まれるサーバ名と透過処理サーバテ

ーブルに記憶されているサーバ名との比較結果に基づいて前記フレームを端末に送出するサーバ情報通知フレーム透過処理手段透過処理手段と、端末から通信経路情報を通知するフレームを受信し、このフレームをネットワークに送出し、ネットワークから通信経路情報を通知するフレームを受信し、そのフレームを端末に送出する通信経路情報中継手段とを有するものである。

【００１０】第３の発明に係わる暗号化装置は、端末からサーバ情報を通知するフレームを受信し、このフレームのサーバ情報に含まれるホップ数に所定の数を加えたフレームをネットワークに送信するホップ数加算手段と、端末から、立ち上がり時の接続相手のサーバ情報を要求するフレームを受信し、所定の接続相手のサーバ情報を通知するフレームを端末に送出する立ち上げ要求応答手段と、ネットワークから、立ち上がり時の接続相手のサーバ情報を要求するフレームを受信し、廃棄する廃棄手段と、端末からのデータフレームを受信し、データフレームの所定のデータ部を暗号化し、ネットワークに送出する暗号化手段と、ネットワークからのデータフレームを受信し、データフレームの所定のデータ部を復号し端末に送出する復号手段と、端末から通信経路情報を通知するフレームを受信し、そのフレームをネットワークに送出し、ネットワークから通信経路情報を通知するフレームを受信し、そのフレームを端末に送出する通信経路情報中継手段とを有するものである。

【００１１】

【発明の実施の形態】

実施の形態１．本実施の形態はクライアントとサーバをネットワークに接続して相互に平文で通信ができると共に、クライアントを暗号化装置を介してネットワークに接続し、またサーバを暗号化装置を介してネットワークに接続して、暗号化装置間は暗号通信ができるようにするものである。パーソナルコンピュータのネットワークＯＳであるＮｅｔＷａｒｅ(Novell社の登録商標)で使用されるプロトコルに適用した例について説明する。

【００１２】ＮｅｔＷａｒｅにおいてはネットワーク層プロトコルとしてＩＰＸ(Internetwork Packet Exchange)プロトコルが使用される。ＩＰＸのフレームを図２に示す。図２において、X1はチェックサム、X2はフレーム長、X3はフレームが経由したルータをカウントするトランスポート制御、X4はフレームの種別を示すフレームタイプ、X5は宛先ネットワーク番号、X6は宛先端末を指定する宛先ノード番号、X7は宛先プロトコルを示す宛先ソケット番号、X8は送信元ネットワーク番号、X9は送信元端末を指定する送信元ノード番号、X10は送信元プロトコルを示す送信元ソケット番号、およびX11はデータ部である。ＩＰＸフレームは宛先ソケット番号X7によってデータ部X11のデータ種別を判別する。

【００１３】ルータ等のネットワークの中継機器は、受信したフレームに示される宛先ネットワークへ中継するためのルーティングテーブルを保持する。受信したフレームの宛先ネットワークと、そのフレームを受信したネットワークが等しくない場合に自分の保持するルーティングテーブルを検索し、テーブル上のルーティング情報に従って受信したフレームを中継する。宛先ネットワークに対するルーティング情報を持たなければそのフレームを中継しない。ルーティング情報はルータやサーバ間でＲＩＰ（Routing Information Protocol）プロトコルを用いて定期的に、あるいは変更があった場合に交換する。ＲＩＰプロトコルはＩＰＸプロトコルの上位に位置し、ＩＰＸヘッダ内の宛先ソケット番号（図２のX7）が0x453（以下０xは１６進数を表わす）であることにより判別する。

【００１４】ＲＩＰのフレームフォーマットを図３に示す。図３においてRP1はオペレーションで、リクエストかまたはレスポンスかを識別する。RP2はネットワーク番号、RP3は目的ネットワークまでに経由するネットワークの数を示すHops数、RP4は目的ネットワークまでにかかる時間を示すTicks数である。Hops数は0x01からカウントし、ルータを通過する毎に１加算される。RP3のHops数が0x10の場合、RP2に示されるネットワークは到達不能を意味し、無効な情報となる。RP2～RP4は１組で１ルーティング情報となり、１フレームの中に複数のルーティング情報が設定可能である。他は図２と同じで説明を省く。

【００１５】また、ＮｅｔＷａｒｅはクライアント／サーバシステムであり、サーバは自分の提供するサービスをブロードキャストする。サーバ情報はルータやサーバ間でＳＡＰ（Service Advertising Protocol）プロトコルを用いて定期的に、あるいは変更があった場合に交換する。ルータやサーバは受信したサーバ情報をサーバテーブルに保持し、受信したリクエストに対してレスポンスを返す。ＳＡＰプロトコルはＩＰＸプロトコルの上位に位置し、ＩＰＸヘッダ内の宛先ソケット番号（図２のX7）が0x452であることにより判別する。

【００１６】ＳＡＰのフレームフォーマットはリクエストフレームとレスポンスフレームの２種類存在する。ＳＡＰのリクエストフレームフォーマットを図４に、ＳＡＰレスポンスフレームフォーマットを図５に示す。図４において、SP1はリクエストタイプ、SP2は要求するサービスタイプである。他は図２と同じで説明を省く。ＳＡＰリクエストフレームはGeneral Requestとクライアントが立ち上り時に送信するNearest Service Queryの２種類があり、リクエストタイプSP1の値により判別される。図５において、SP3はレスポンスタイプ、SP4はサービスタイプ、SP5はサーバ名、SP6はサーバのアドレスであるネットワーク番号、SP7はノード番号、SP8はソケット番号、SP9はサーバまでの中継ネットワーク数を示すHops数である。他は図２と同じで説明を省く。

【００１７】SP9のHops数が0x10の場合、サーバ名SP5に

示されるサーバは使用不能であることを示す。レスポンスフレームはリクエストに対するレスポンスと定期的にサーバ情報をブロードキャストするフレームの２種類あり、レスポンスタイプSP3により判別される。SP4～SP8は１組で１サーバのサーバ情報を構成し、１フレームの中に複数のサーバ情報を設定できる。

【００１８】本実施の形態は、暗号化装置がプロトコルを判別し、ＮｅｔＷａｒｅにおけるＲＩＰフレームとＳＡＰフレームを暗号化せずに透過し、ＳＡＰフレームに含まれるサーバのサービスタイプを暗号サービスの値に変更して送信し、そのサーバ情報を含むＳＡＰフレームを受信した暗号化装置が元の非暗号サービスのサービスタイプに戻す。その他のデータフレームは図２に示したデータ部X11を暗号化する。暗号化装置の構成を図１に示す。図１において、1は端末、2は暗号化装置、3はネットワークである。21は端末側送受信部で、１つ以上のポートを持ち、ポートに接続された端末と装置の間のデータの送受信を行う。23はネットワーク側送受信部で、ネットワークと装置の間のデータの送受信を行う。22は受信したフレームを格納しておくフレーム格納メモリ、24はプログラム及び作業用のＲＯＭ／ＲＡＭ、25は各種の演算処理を行う中央処理部である。26は受信したデータのプロトコルを判別するプロトコル判別部、27は受信したデータの暗号／復号処理を行うデータ暗号／復号処理部、28はＳＡＰ処理部で、端末からのＳＡＰフレームなら、サービスタイプを非暗号サービスから暗号サービスに変更し、ネットワークからのＳＡＰフレームなら、暗号サービスから非暗号サービスに変更する。

【００１９】動作について説明する。図１において、暗号化装置の端末側送受信部21は、受信したフレームをフレーム格納メモリ22に格納する。ネットワーク側送受信部23は、受信したフレームをフレーム格納メモリ22に格納する。プロトコル判別部26はフレームのプロトコルを判別し、ＲＩＰフレームであれば透過し、ＳＡＰフレームであればＳＡＰ処理部28へ制御を渡す。ＳＡＰ処理部28は端末1からＳＡＰフレームを受信した場合はサービスタイプ0x04（非暗号サービス）を例えば0xabc（暗号サービス）に変換して、ネットワーク側送受信部23を介してネットワーク3に送信し、ネットワーク3からSAPフレームを受信した場合はサービスタイプ0xabcを0x04に変換し、Hops数を0x10に設定して、端末側送受信部21を介して端末側1に送信する。

【００２０】その他のデータフレームのデータ部（図２のX11）はデータ暗号／復号処理部27において暗号化／復号処理する。ネットワーク側送受信部23は、それぞれ処理したフレームをネットワーク3へ送信する。また、フレームを送信した端末以外の端末へは端末側送受信部21より受信したフレームをそのまま送信する。ネットワーク側送受信部23から受信したフレームも同じように処理し、端末側送受信部21より端末側1へ送信する。

【００２１】次に、同一ネットワーク上のクライアント／サーバが暗号化せずに通信する場合のネットワーク構成例を図６に示す。図６において、３ａはネットワーク、11s、12sはサーバ、11cはクライアントである。５１はサーバ11sが保持するサーバテーブル、５２はサーバ12sが保持するサーバテーブルで、それぞれサーバ名とサービスタイプ等のサーバ情報を保持している。次にサーバが自分のサーバ情報を定期的に送信するシーケンスを図７に示す。図において、ファイルサーバ11sはＳＡＰフレームを用いて定期的に自分のサーバ情報(サーバ名11s、サービスタイプ0x04)をネットワーク3a上にブロードキャストに送信する（ステップS11）。ネットワーク3aからＳＡＰフレームを受信したファイルサーバ12sはＳＡＰフレームに含まれるサーバ名11s、サービスタイプ0x04をサーバテーブル５２に設定する（ステップS12）。

【００２２】ファイルサーバ12sはＳＡＰフレームを用いて定期的に自分のサーバ情報(サーバ名12s、サービスタイプ0x04)をネットワーク3a上にブロードキャストに送信する（ステップS13）。ネットワーク3aからＳＡＰフレームを受信したファイルサーバ11sはＳＡＰフレームに含まれるサーバ名12s、サービスタイプ0x04をサーバテーブル５１に設定する（ステップS14）。次に、クライアント11c立ち上がり時のシーケンスを図８に示す。図において、クライアント11cは、立ち上がり時にサービスタイプ0x04のNearest ServiceQueryのＳＡＰリクエストフレームをネットワーク3aに送信する（ステップＳ２１）。

【００２３】サーバ１１ｓは、ネットワーク3aからサービスタイプ0x04のSAPリクエストを受信すると（ステップS22）、自サービスタイプと同一なので、自分のサーバ情報（サーバ名11s、サービスタイプ0x04）のSAPレスポンスフレームをクライアント11cに送信する（ステップS23）。クライアント11cは最初にレスポンスフレームをファイルサーバ11sから受信すると（ステップS24）、レスポンスフレームに設定されているサーバ11sのルーティング情報を得るために、ＲＩＰリクエストフレームを送信する（ステップS31）。

【００２４】サーバ11sはＲＩＰリクエストフレームを受信すると（ステップS32）、レスポンスを送信する（ステップS33）。クラアント11cはＲＩＰレスポンスフレームを受信すると（ステップS34）、以後クラアント11cとサーバ11s間でデータフレームを送受信する（ステップS41、S42）。なお、ファイルサーバ12sはネットワーク3aからリクエストフレームを受信し（ステップS25）、サービスタイプが自サービスタイプと同一のサーバ12sは、自分のサーバ情報（サーバ名12s、サービスタイプ0x04）のSAPレスポンスフレームを送信すると（ステップS26）クライアント11cはこの後から遅れて受信したレスポンスフレームを無視する（ステップS27）。

【００２５】上述のように、図８のS21で送信するＳＡＰリクエストフレームはブロードキャストするためサーバ12sも受信し、レスポンスを送信する。クライアントはＳＡＰレスポンスを複数受信した場合、一番最初に受信したレスポンスフレームに従ってデータ通信を開始する。また、例えばサーバ11sに接続したクライアント11cがサーバ12sともデータ通信を行ないたい場合、クライアント11cは接続されているサーバ11sからサーバ12sのアドレス情報を得るために、ＲＩＰリクエストを送信し、これに対するＲＩＰレスポンスの応答からアドレス情報を得て、クライアント11cはサーバ12sと通信を開始する。なお、サーバ11sからサーバ12sのアドレス情報が得られない場合は通信できない。

【００２６】次にルータを介して異なるネットワーク上のクライアント／サーバが、暗号化せずに通信する場合のネットワーク構成例を図９に示す。図において、3a、3bはネットワーク、4aはルータ、11sはサーバ、11cはクライアント、51はルータ4aが保持するサーバテーブル、52はサーバ11sが保持するサーバテーブルである。サーバ11sが自分のサーバ情報を含むレスポンスフレームを定期的にネットワーク3bに送信するシーケンスを図１０に示す。図１０においてファイルサーバ11sはＳＡＰフレームを用いて定期的に自分の情報をネットワーク3b上にブロードキャストする（ステップS11）。ルータ4aはサーバ情報を受信すると（ステップS12）自分のサーバテーブル51に登録し、他のネットワーク3aへ定期的に送信する（ステップS13）。

【００２７】クライアント11cの立ち上がり時のシーケンスを図１１に示す。図において、クライアント11cがサービスタイプ0x04のNearest Service QueryのSAPリクエストフレームをネットワーク3aへ送信する（ステップS21）。ルータ4aはNearestService QueryのSAPリクエストフレームを受信する（ステップS22）と、サーバテーブル51を参照して、要求されたサービスタイプで（0x04で）Hops数が最少のサーバ名11sのファイルサーバ情報を設定したレスポンスフレームをクライアント11cに送信する（ステップS23）。クライアントは受信したレスポンスフレーム（ステップS24）に設定されているサーバのルーティング情報を得るために、ＲＩＰリクエストフレームを送信する（ステップS31）。ＲＩＰリクエストフレームを受信したルータ（ステップS32）はレスポンスを送信する（ステップS33）クライアント11cは受信したＲＩＰレスポンスフレームに従い（ステップS34）、通信を開始する（ステップS41、S42、S43）。

【００２８】次に、同一ネットワーク上に暗号系サーバ／クライアント、非暗号系サーバ／クライアントが存在するネットワークシステム構成図を図１２に示す。図１２において、2a、2b、2cは暗号化装置、3aはネットワーク、11cは暗号化装置が接続されていない非暗号系クライアント、12cは暗号化装置が接続された暗号系クライアント、11sは暗号化装置が接続されていない非暗号系サーバ、12s、13sは暗号化装置が接続された暗号系サーバを示す。52はサーバ11sが保持するサーバテーブル、53はサーバ12sが保持するサーバテーブル、54はサーバ13sが保持するサーバテーブルで、サーバ名、サービスタイプ、Hops数などのサーバ情報を記憶する。

【００２９】図１２に示すネットワーク構成において、非暗号系サーバ11s、暗号系サーバ12s、13sは定期的に自分のサーバ情報をネットワーク3a上にブロードキャストに送信し、各サーバが他サーバからのサーバ情報を受信して自サーバテーブルを更新するシーケンスを図１３に示す。図１３において、非暗号系サーバ11sはネットワーク3aにサーバ名11sでサービスタイプ0x04のサーバ情報をブロードキャストする（ステップS11）。

【００３０】暗号化装置2bはネットワーク3aから前記サーバ11sのサーバ情報を受信するとサービスタイプ0x04で、Hops数を0x10（サーバ11sが使用不能を示す値）に設定し、サーバ12sへ送信する（ステップS12）。サーバ12sは暗号化装置2bからサーバ11sのサーバ情報を受信すると、サーバ情報のHops数が0x10であるので、そのサーバ情報を廃棄しサーバ12sのサーバテーブル53にはサーバ11sのサーバ情報は書込まない（ステップS13）。同様にして、暗号化装置2cはネットワーク3aから前記サーバ11sのサーバ情報を受信すると、サービスタイプが0x04なのでHops数を0x10に設定し、サーバ13sへ送信する（ステップS14）。サーバ13sは暗号化装置2cからサーバ11sのサーバ情報を受信すると、サーバ情報のHops数が0x10であるので、そのサーバ情報を廃棄し、サーバ13sのサーバテーブル54にはサーバ11sのサーバ情報は書き込まない（ステップS15）。

【００３１】次に、暗号系サーバ12sはサーバ名12s、サービスタイプ0x04のサーバ情報をブロードキャストに送信する（ステップS21）。暗号化装置2bは暗号系サーバを示すサービスタイプ0xabcに変更してネットワーク3aに送信する（ステップS22）。ネットワーク3aからサーバ12sのサーバ情報を受信した非暗号系サーバ11sは自サーバが保持するサーバテーブル52にサーバ名12sとサービスタイプ0xabcを登録する（ステップS23）。また、暗号化装置2cはネットワーク3aからサーバ12sのサーバ情報を受信すると、受信したサーバ情報のサービスタイプ0xabcを0x04に変更してサーバ13sに出力する（ステップS24）。サーバ13sはサーバ12のサーバ情報を暗号化装置2cから受信すると自サーバが保持するサーバテーブル54にサーバ名12sとサービスタイプ0x04を登録する（ステップS25）。

【００３２】次に、暗号系サーバ13sは暗号化装置2cにサーバ名13s、サービスタイプ0x04のサーバ情報を送信する（ステップS31）。暗号化装置2cは暗号系サーバを示すサービスタイプ0xabcに変換してネットワーク3aに送信する（ステップS32）。ネットワーク3aからサーバ1

3sのサーバ情報を受信した非暗号系サーバ11sは自サーバが保持するサーバテーブル51にサーバ名13sとサービスタイプ0xabcを登録する（ステップS33）。暗号化装置2bはネットワーク3aからサーバ13sのサーバ情報を受信すると受信したサーバ情報のサービスタイプ0xabcを0x04に変換してサーバ12sに送信する（ステップS34）。サーバ12sはサーバ13sのサービス情報を暗号化装置2bから受信すると、自サーバが保持するサーバテーブル53にサーバ名とサービスタイプ0x04を登録する（ステップS35）。以上のように、サーバは定期的に互いのサーバ情報を更新する。

【００３３】図１２のシステムにおいて、暗号系クライアント12cが立ち上がって暗号系サーバ12sと通信を開始するまでのシーケンスを図１４を用いて説明する。暗号系クライアント12cは暗号化装置2aにサービスタイプ0x04のNearest Service QueryのＳＡＰリクエストフレームを送信する（ステップS21）。暗号化装置2aは、サービスタイプ0x04のNearest Service QueryのＳＡＰリクエストフレームを受信すると、0x04のサービスタイプを0xabcに変更してネットワーク3aへ送信する（ステップS22）。非暗号系サーバ11sは自分のサービスタイプと異なるため、リクエストを廃棄する（図示せず）。暗号化装置2bは、ネットワーク3aからサービスタイプ0xabcのNearest Service QueryのＳＡＰリクエストを受信すると、0x04に変更して暗号系サーバ12sへ送信する（ステップS23）。

【００３４】暗号系サーバ12sは、サービスタイプ0x04のNearest Service QueryのＳＡＰリクエストを受信する（ステップS24）と、自サービスタイプと同じなので、サーバ12sはサーバ名12sでサービスタイプ0x04の自分のサーバ情報をレスポンスとして送信する（ステップS25）。暗号化装置2bは、ネットワーク3aからサーバ名12sでサービスタイプ0x04のレスポンスを受信すると、サービスタイプ0xabcに変更してネットワーク3aへ送信する（ステップS26）。暗号化装置2aはネットワーク3aからサービスタイプ0xabcのレスポンスを受信すると0x04に変更して暗号系クライアント12cへ送信する（ステップS27）。暗号系クライアント12cは受信したサーバ（ステップS28）のアドレスを得るためにＲＩＰリクエストフレームを送信する（ステップS31）。暗号化装置2aは受信したＲＩＰリクエストをそのまま送信する（ステップS32）。

【００３５】暗号化装置2bはネットワーク3aから受信したＲＩＰリクエストをそのまま暗号系サーバ12sに送信する（ステップS33）。暗号系サーバ12sはＲＩＰリクエストを受信し（ステップS34）、ＲＩＰレスポンスを暗号化装置2bに送信する（ステップS35）。暗号化装置2bは受信したＲＩＰレスポンスをそのままネットワーク3aに送信する（ステップS36）。暗号化装置2aはネットワーク3aから受信したＲＩＰレスポンスをそのまま暗号系クライアント12cに送信する（ステップS37）。暗号系クライアント12cは受信したＲＩＰレスポンスに従い（ステップS38）、暗号系サーバ12sとデータフレームの送受信を開始する。すなわち、暗号系クライアント12cはサーバ12s宛にデータフレームを送信する（ステップS41）。暗号化装置2aは受信したデータフレームのデータ部X11を暗号化し、ネットワーク3aへ送信する（ステップS42）。暗号化装置2bは受信したデータフレームのデータ部X11を復号し、暗号系サーバ12sへ送信し（ステップS43）、暗号系サーバがデータフレームを受信する（ステップS44）。また、暗号系サーバ12sから暗号系クライアント12cへはステップS41からステップS44の逆をたどってデータが送信される。

【００３６】図１２に示すシステムにおいて、暗号系クライアント12cが立ち上がり時に送信するＳＡＰリクエストを非暗号系サーバ11sが受信した場合のシーケンスを図１５に示す。図１５において、暗号系クライアント12cが立ち上がり時にサービスタイプ0x04のNearest Service QueryのＳＡＰリクエストフレームを送信すると（ステップS21）、暗号化装置2aはサービスタイプを0xabcに変更してネットワーク3aに送信する（ステップS22）。非暗号系サーバ11sはネットワーク3aからサービスタイプを0xabcのNearest Service QueryのＳＡＰリクエストフレームを受信すると、非暗号系サーバ11sは自分のサービスタイプ0x04と異なるため、リクエストを廃棄する（ステップS23）。

【００３７】逆に非暗号系クライアント11cが立ち上がる時に送信するＳＡＰリクエストを暗号系サーバ12sを収容する暗号化装置2bが受信した場合のシーケンスを図１６に示す。図１６において、非暗号系クライアント11cが立ち上がり時にサービスタイプ0x04のNearest Service QueryのＳＡＰリクエストフレームを送信すると（ステップS21）、このＳＡＰリクエストフレームを受信した暗号化装置2bはサービスタイプが0xabcと異なるためリクエストを廃棄する（ステップS22）。従って、非暗号系クライアントを暗号系サーバに、また暗号系クライアントを非暗号系サーバに接続できない。

【００３８】次に、同一ネットワーク上に暗号系サーバ、非暗号系サーバが存在し、ルータを介して異なるネットワーク上に暗号系クライアント、非暗号系クライアントが存在するネットワークシステム構成図を図１７に示す。図１７において、3a、3bはネットワーク、4aはルータ、2a、2b、2cは暗号化装置、11sは非暗号系サーバ、12s、13sは暗号系サーバ、12cは暗号系クライアント、11cは非暗号系クライアント、51はルータ4aが保有するサーバテーブル、52はサーバ11sが保有するサーバテーブル、53はサーバ12sが保有するサーバテーブルである。なお、サーバ13sが保有するサーバテーブルについての説明は省略する。

【００３９】図１２の例と同様に、非暗号系サーバ11

s、暗号系サーバ12s、13sはＳＡＰフレームを用いて定期的に自分のサーバ情報をネットワーク上にブロードキャストに送信し、非暗号系サーバ11s、暗号系サーバ12s、13sは受信したＳＡＰフレームによりサーバ情報を学習する（図１７の52、53）。ルータ4aはネットワーク3bから受信した非暗号系サーバ11s、暗号系サーバ12s、13sのＳＡＰフレームをもとにサーバ情報をサーバテーブル51に登録する。即ち、サーバ11sのＳＡＰフレームはサーバ名11s、サービスタイプ0x04を登録し、サーバ12sのＳＡＰフレームはサーバ名12s、サービスタイプ0xabcを登録し、サーバ13sのＳＡＰフレームはサーバ名13s、サービスタイプ0xabcを登録する。暗号系クライアント12cが立ち上がり、暗号系サーバ12sと通信を開始するまでのシーケンスを図１８に示す。図において、暗号系クライアント12cは立ち上がり時にサービスタイプ0x04のNearest Service QueryのＳＡＰリクエストを送信する（ステップS21）。暗号化装置2aは、クライアント側からサービスタイプ0x04のＳＡＰリクエストを受信すると、サービスタイプを0xabcに変更してネットワーク3aへ送信する（ステップS22）。

【００４０】ルータ4aは、サービスタイプ0xabcのＳＡＰリクエストを受信すると（ステップS23）、サーバテーブル51を参照しＳＡＰリクエストと同じサービスタイプ0xabcで最小のHops数のサーバ名12sを求め暗号系サーバ12sの情報をＳＡＰレスポンスとして送信する（ステップS24）。暗号化装置2aはネットワーク側からサービスタイプ0xabcのサーバ情報を受信すると、0x04に変更して暗号系クライアント12cへ送信し（ステップS25）、暗号系クライアント12cが受信する（ステップS26）。暗号系クライアント12cは受信したサーバ12sのアドレスを得るためにＲＩＰリクエストを送信する（ステップS31）。暗号化装置2aはＲＩＰフレームをそのままネットワーク3aへ送信する（ステップS32）。

【００４１】ルータ4aはネットワーク3aから暗号化装置2aのＲＩＰリクエストを受信し（ステップS33）、レスポンスをネットワーク3aへ送信する（ステップS34）。暗号化装置2aはネットワーク3aからのＲＩＰレスポンスをそのまま暗号系クライアント12cへ送信し（ステップS35）、暗号系クライアント12cがＲＩＰレスポンスを受信する（ステップS36）。暗号系クライアント12cは暗号系サーバ宛に通信を開始する（ステップS41）。即ち、暗号化装置2aはデータフレームのデータ部X11を暗号化して送信する（ステップS42）。ルータ4aはルーティングテーブルに従い、宛先アドレス宛にフレームを送信する（ステップS43）。暗号化装置2bは受信したデータフレームのデータ部X11を復号して送信し（ステップS44）、暗号系サーバが復号されたデータフレームを受信する（ステップS45）。また、暗号系サーバ12sから暗号系クライアント12cへはステップS41からステップS45の逆をたどってデータが送信される。暗号系サーバ12sは自サーバテーブル53に非暗号系サーバ11sの情報を保持しないため、暗号系クライアント12cは非暗号系サーバ11sへアクセスできない。

【００４２】このように、ＲＩＰ／ＳＡＰフレームは暗号化せず、サーバのサービスタイプを暗号系と非暗号系に分け、その他のデータフレームは暗号化することにより、暗号系クライアント／サーバと非暗号系クライアント／サーバが混在するネットワーク上で暗号通信が可能となる。

【００４３】さらに同一ネットワーク上で暗号系サーバのサービスタイプとして割り当てる値を複数使用することにより、閉域の暗号グループを構成することができる。システム構成を図１９に示す。図１９において、11cは非暗号系クライアント、12c、13cは暗号系クライアント、11sは非暗号系ファイルサーバ、12s、13sは暗号系ファイルサーバを示す。暗号化装置2a、2bには変換するサービスタイプとして0xabcを設定し、暗号化装置2c、2dには0xdefを設定することにより同一サービスタイプのクライアントとサーバが相互に通信できる。従って暗号系サービスタイプを暗号鍵に対応付ければ、複数の暗号グループを構成できる。

【００４４】本実施の形態ではＮｅｔＷａｒｅに適用した例を示したが、ルーティング情報を交換してフレームの中継を行い、サーバ情報を交換してクライアントがサーバに接続し、サーバ／クライアント間で定期的に接続を確認するその他のプロトコルに対しても同様の効果を奏する。

【００４５】実施の形態２．実施の形態１ではサービスタイプにより暗号／非暗号の区別していたが、本実施の形態はこのほかにクライアントを収容する暗号化装置が、宛先サーバ対応に暗号化／復号を行なうか否かを指定する透過処理アドレステーブルと、サーバを収容する暗号化装置に、非暗号のサーバを記憶する透過処理サーバテーブルを設けることにより、暗号化装置に接続されたクライアントと非暗号のサーバとを接続できるようにするものである。

【００４６】ＮｅｔＷａｒｅにおいて、クライアントは立ち上がり時にサーバに接続し、そのサーバをベースサーバとして、複数のサーバとコネクションをはり、通信を行うことができる。クライアントが他のサーバとコネクションを張る場合、サーバ名を指定し、ベースサーバからコネクション先サーバのアドレス情報（図５のネットワーク番号SP6、ノード番号SP7）を得る。アドレス情報受信後、そのネットワーク番号SP6に対するＲＩＰリクエストを送信する。クライアントはＲＩＰレスポンス受信後、サーバとコネクションを張る。ベースサーバがコネクション先サーバのアドレス情報を保持していなければ、コネクションを張ることができない。本実施の形態では、暗号化装置に宛先アドレスによって暗号化／復号を行うか否かの設定をすることにより、暗号化装置が

接続されているクライアントと暗号化装置が接続されていないサーバとの間で非暗号の通信ができるようにするものである。

【００４７】本実施の形態の暗号化装置の構成を図２０に示す。図２０において、30は透過処理アドレステーブル、31は透過処理サーバテーブルである。27はデータ暗号／復号処理部で、データフレームに含まれる通信相手のサーバアドレスが透過処理アドレステーブル30登録されているなら暗号化／復号せず、登録されていないなら暗号化／復号する。28はＳＡＰ処理部で、ネットワーク側から受信したＳＡＰフレームに含まれるサーバ情報のサーバが透過処理サーバテーブル31に登録されていればＳＡＰフレームをそのまま送信し、登録されていなければ廃棄する。図２０の1から3，21から26は実施の形態１（図１）と同じであり、説明を省略する。次に、通信システムの構成を図２１に示す。図において、30aは透過処理アドレステーブル（図２０の30）で、宛先サーバアドレスを記憶し、クライアントを収容する暗号化装置2aが保持する。この例では透過処理アドレステーブル30aに宛先サーバアドレス11sを保持しており、暗号化装置2aがサーバ11s宛のフレームを暗号化／復号しないことを意味する。

【００４８】31bは透過処理サーバテーブル（図２０の31）で、サーバ名を記憶し、サーバを収容する暗号化装置2bが保持する。この例では暗号化装置2bが透過処理サーバテーブル31bにサーバ名11sを保持している。サーバ名11sが透過処理サーバテーブル31bに登録されていることは、暗号化装置がサーバ11sからのＳＡＰレスポンスフレームのサービスタイプを変更せず、Hops数も変更せず、透過処理することを意味する。また、暗号化装置2cには透過処理するサーバがないので、透過処理サーバテーブル31cにサーバ名を記憶していない。なお、11sは非暗号サーバ、12sはサーバタイプ0xabcの暗号サーバ、13sはサーバタイプ0xdefの暗号サーバである。11c、12c、13c、11s、12s、13s、3a、3b、4a、51、52、53、54は図１９と同じであり、説明を省略する。

【００４９】図２１のシステムにおいて、サーバ11s、12s、13sが定期的に自分のサーバ情報を送信するシーケンスを図２２に示す。図において、サーバ11sは自分の情報を定期的にブロードキャストに送信する（ステップS11）。暗号化装置2bはネットワーク側送受信部よりサーバ11sの情報を受信し、フレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）に渡す。プロトコル判別部においてＳＡＰフレームと判別され、ＳＡＰ処理部（図２０の28）に渡す。ＳＡＰ処理部において透過処理サーバテーブル31b（図２０の31）を検索し、サーバ11sが登録されているので、そのまま端末側送受信部（図２０の21）より送信する（ステップS12）。サーバ12sはサーバ11sの情報を受信し、サーバ名11s、サービスタイプ0x04をサーバテーブル53に登録する（ステップS13）。

【００５０】暗号化装置2cはネットワーク側送受信部（図２０の23）よりサーバ11sの情報を受信し、フレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）に渡す。プロトコル判別部においてＳＡＰフレームと判別され、ＳＡＰ処理部（図２０の28）に渡す。ＳＡＰ処理部において透過処理サーバテーブル31c（図２０の31）を検索し、サーバ11sが登録されていないため、Hops数を0x10（無効なサーバ情報）に変更し、端末側送受信部（図２０の21）より送信する（ステップS14）。サーバ13sはHops数が無効な値、0x10なので、サーバ11sの情報を廃棄する（ステップS15）。

【００５１】サーバ12sは自分の情報を定期的にブロードキャストに送信する（ステップS16）。暗号化装置2bは端末側送受信部よりサーバ12sの情報を受信し、フレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）に渡す。プロトコル判別部においてＳＡＰフレームと判別され、ＳＡＰ処理部（図２０の28）に渡す。ＳＡＰ処理部においてサービスタイプを0xabcに変更し、端末側送受信部（図２０の21）より送信する（ステップS17）。サーバ11sはサーバ12sの情報を受信し、サーバ名12s、サービスタイプ0xabcとしてサーバテーブル52に登録する（ステップS18）。

【００５２】暗号化装置2cはネットワーク側送受信部（図２０の23）よりサーバ12sの情報を受信し、フレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）に渡す。プロトコル判別部においてＳＡＰフレームと判別され、ＳＡＰ処理部（図２０の28）に渡す。ＳＡＰ処理部においてそのまま送信と判定し、端末側送受信部（図２０の21）よりそのまま送信する（ステップS19）。サーバ13sはサーバ12sの情報を受信し、サーバ名12s、サービスタイプ0xabcとしてサーバテーブル54に登録する（ステップS20）。サーバ13sはサーバ12sと同様のシーケンスにより、自分のサーバ情報であるサーバ名13sとサービスタイプ0xdefを定期的にブロードキャストに送信し、サーバ11sはサーバテーブル52に、サーバ12sはサーバテーブル53に登録する。

【００５３】暗号系クライアントが、暗号系サーバをベースサーバとして、非暗号系サーバと通信を行うシーケンスを図２３に示す。図において、暗号系クライアント12cは立ち上がり時に図１８に示したシーケンス（ステップS21）をたどり、暗号系サーバ12sに接続する。クライアント12cはベースサーバ12sからコネクションを張るサーバ11sのアドレス情報に対するリクエストをデータフレームのデータ部X11にサーバ11sのアドレスに対するRequestを設定してサーバ12sへ送信する（ステップS51）。

【００５４】暗号化装置2aは端末側送受信部（図２０の21）から受信したフレームをフレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）に

おいてデータフレームと判断し、データ暗号／復号処理部（図２０の27）へ渡す。データ暗号／復号処理部において透過処理アドレステーブル30a（図２０の30）を検索し、ベースサーバ12sが登録されていないのでデータ部X11を暗号化し、ネットワーク側送受信部（図２０の23）より送信する（ステップS52）。ルータ4aはデータフレームを中継する（ステップS53）。

【００５５】暗号化装置2bはネットワーク側送受信部（図２０の23）から受信したフレームをフレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）においてデータフレームと判断し、データ暗号／復号処理部（図２０の27）へ渡す。データ暗号／復号処理部において、（サーバを収容する暗号化装置は透過処理アドレステーブル30を持たないので）データ部X11を復号し、端末側送受信部（図２０の21）より端末へ送信する（ステップS54）。ベースサーバ12sはサーバ11sのアドレスに対するRequestを受信すると（ステップS55）、自分のサーバテーブル53を検索し、保持するサーバ11sのサーバ情報を求めサーバ11sのアドレスに対するResponseを送信する（ステップS56）。

【００５６】暗号化装置2bは端末側送受信部（図２０の21）から受信したフレームをフレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）においてデータフレームと判断し、データ暗号／復号処理部（図２０の27）へ渡す。データ暗号／復号処理部において、（サーバを収容する暗号化装置は透過処理アドレステーブル30を持たないので）データ部X11を暗号化し、端末側送受信部（図２０の21）より端末へ送信する（ステップS57）。

【００５７】ルータ4aは受信したデータフレームを中継する（ステップS58）。暗号化装置2aはネットワーク側送受信部（図２０の23）から受信したフレームをフレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）においてデータフレームと判断し、データ暗号／復号処理部（図２０の27）へ渡す。データ暗号／復号処理部において透過処理アドレステーブル30a（図２０の30）を検索し、サーバ12sが登録されていないのでデータ部X11を復号し、端末側送受信部（図２０の21）より端末へ送信する（ステップS59）。クライアント12cはサーバ11sの情報を得て（ステップS60）、サーバ11sのアドレスに対するＲＩＰリクエストを送信する（ステップS31）。

【００５８】暗号化装置2aは端末側送受信部（図２０の21）から受信したフレームをフレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）においてＲＩＰフレームと判断し、ネットワーク側送受信部（図２０の23）より端末へ送信する（ステップS32）。ルータ4aはＲＩＰリクエストを受信すると（ステップS33）、ルーティングテーブルを検索し、レスポンスを送信する（ステップＳ３４）。暗号化装置２ａはネットワーク側送受信部（図２０の23）から受信したフレームをフレーム格納メモリ（図２０の22）に格納し、プロトコル判別部（図２０の26）においてＲＩＰフレームと判断し、端末側送受信部（図２０の21）より端末へ送信する（ステップS35）。クライアント12cはＲＩＰレスポンスを受信する（ステップS36）。暗号系クライアント12cは非暗号系サーバ11s宛に通信を開始する（ステップS46）。

【００５９】暗号化装置2aは非暗号系サーバ11s宛のフレームを端末側送受信部より受信するとフレーム格納メモリ（図２０の22）に格納する。フレーム格納メモリに格納されたフレームはプロトコル判別部（図２０の26）においてデータフレームと判別され、データ暗号／復号処理部（図２０の27）に渡される。データ暗号／復号処理部において透過処理アドレステーブル30a（図２０の30）を検索し、サーバ11sのアドレスが登録されているので、データ部X11をそのまま暗号化せず、ネットワーク側送受信部（図２０の23）より送信する（ステップS47）。サーバ11sより受信したフレームも透過処理アドレステーブル30aにサーバ11sが登録されているので、暗号化装置2aは復号せずそのままデータフレームをネットワーク3aに送信し、ルータ4aはネットワーク3bへ中継する（ステップS48）。非暗号系サーバ11sはネットワーク3bから受信したデータフレームを受信する（ステップS49）。このように暗号系クライアント12cは暗号系サーバ12sとは暗号通信し、非暗号系サーバ11sとは非暗号通信が可能となる。

【００６０】実施の形態３．実施の形態１ではサービスタイプによって暗号／非暗号を区別していたが、本実施の形態はHops数の大小により暗号・非暗号を区別しようとするものである。暗号化装置の構成を図２４に示す。図２４において、32はHops数メモリで、端末側から受信したＳＡＰレスポンスに加算するHops数を記憶する。33はサーバ情報テーブルで、端末側から受信したNearest Service QueryのＳＡＰリクエストに対して予め登録しておいた接続相手のサーバ情報を格納するテーブルである。28はＳＡＰ処理部で、端末側からNearest Service QueryのＳＡＰリクエストを受信した場合、サーバ情報テーブル33に記憶しているサーバ情報をＳＡＰレスポンスとして端末側に送出し、ネットワークからNearest Service QueryのＳＡＰリクエストを受信した場合はそのＳＡＰリクエストを廃棄する。また、ＳＡＰ処理部33は端末側からＳＡＰレスポンスを受信した場合、ＳＡＰレスポンスに含まれるHops数をHops数メモリ32の内容を加えてネットワーク側に送信する。他は図１と同じで説明を省く。

【００６１】ネットワークシステム構成を図２５に示す。図２５において、11c、12c、11s、12s、13s、2a、2b、2c、3a、3b、4a、51、52、53は図２１と同じである。33は図２４の33と同じで、暗号化装置2aのNearest

Service QueryのＳＡＰリクエストに対するサーバ情報テーブルであり、即ち立ち上げ時に接続するサーバのサーバ情報を記憶するテーブルであり、本実施の形態では暗号化装置2aの端末からのNearest Service Queryに対するサーバ情報に暗号系サーバ12sの情報（サーバ名12s、サービスタイプ0x04、Hops数0x02）を登録した場合の例を示す。32は図２４の32と同じで、暗号化装置2bのＳＡＰレスポンスに対して加算するHops数を記憶するHops数メモリを示し、本実施の形態では５を登録した例を示す。

【００６２】動作について説明する。図２５のネットワークシステム構成において、サーバ11s、12s、13sが定期的にサーバ情報を送信するシーケンスを図２６に示す。図において、非暗号系サーバ11sは、サーバ名11s、サービスタイプ0x04、Hops数0x01のサーバ情報を定期的にブロードキャストに送信する（ステップS11）。暗号化装置2bはネットワーク側送受信部（図２４の23）から受信したフレームをフレーム格納メモリ（図２４の22）に格納し、プロトコル判別部（図２４の26）においてＳＡＰフレームと判断し、ＳＡＰ処理部（図２４の28）へ渡す。ＳＡＰ処理部においてそのまま送信と判断し、端末側送受信部（図２４の21）より端末、即ち暗号サーバ12sへ送信する（ステップS12）。

【００６３】暗号系サーバ12sはサーバ情報を受信し、サーバ名11s、サービスタイプ0x04、Hops数0x01のサーバ情報をサーバテーブル53に登録する（ステップS13）。暗号化装置2cは暗号化装置2bと同様にフレームをそのまま暗号系サーバ13sへ送信する（ステップS14）。暗号系サーバ13sはサーバ情報を受信し、サーバ名11s、サービスタイプ0x04、Hops数0x01のサーバ情報をサーバテーブルに登録する（ステップS15）。暗号系サーバ12sはサーバ名12s、サービスタイプ0x04、Hops数0x01の自分のサーバ情報を定期的にブロードキャストに送信する（ステップS16）。

【００６４】暗号化装置2bは端末側送受信部（図２４の21）から受信したフレームをフレーム格納メモリ（図２４の22）に格納し、プロトコル判別部（図２４の26）においてＳＡＰフレームと判断し、ＳＡＰ処理部（図２４の28）へ渡す。ＳＡＰ処理部（図２４の28）において端末からのファイルサーバ情報にHops数メモリ32に登録されているHops数（この例では５）をＳＡＰレスポンスフレームのHops数（図５のSP9）に加算し、ネットワーク側送受信部（図２４の21）よりネットワーク3bへ送信する（ステップS17）。非暗号系サーバ11sはサーバ名12s、サービスタイプ0x04、Hops数0x06のサーバ情報を受信し、サーバテーブル52に登録する（ステップS18）。暗号化装置2cは受信したサーバ情報をＳＡＰ処理部（図２４の28）によりそのまま送信と判断し、サーバ13sへ送信する（ステップS19）。

【００６５】暗号系サーバ13sはサーバ情報を受信し、サーバ名12s、サービスタイプ0x04、Hops数0x06のサーバ情報をサーバテーブルに登録する（ステップS20）。暗号系サーバ13sは、暗号系サーバ12sのサーバ情報受信と同様のシーケンスにより、自分のサーバ情報を定期的にブロードキャストに送信する。サーバ11sはサーバ名13s、サービスタイプ0x04、Hops数0x06のサーバ情報をサーバテーブル52に登録する。サーバ12sはサーバ名13s、サービスタイプ0x04、Hops数0x06のサーバ情報をサーバテーブル53に登録する。（ステップS21～ステップS25）

なお、図２６でルータ4aの説明を省略したが、ルータ4aはネットワーク3bから受信したサーバ情報をもとにサーバテーブル51を更新する。即ち、サーバ11sからのサーバ名11s、サービスタイプ0x04、Hops数0x01のサーバ情報をネットワーク3bから受信してサーバテーブル51に登録する。

【００６６】また、12sからのサーバ名12s、サービスタイプ0x04、Hops数0x06のサーバ情報をネットワーク3bから受信してサーバテーブル51に、またサーバ13sからのサーバ名13s、サービスタイプ0x04、Hops数0x06のサーバ情報をネットワーク3bから受信してサーバテーブル51に登録する。このように、ネットワーク上のサーバおよびルータは図２５の51、52、53に示したようにサーバ情報を学習する。

【００６７】図２５のネットワークシステムにおいて非暗号系クライアント11c立ち上がり時のシーケンスは図１１と同じである。図１１において、ルータ4aはクライアント11cからNearest Service QueryのＳＡＰリクエストを受信すると、保持するサーバテーブル51の中でHops数の最少のサーバ情報を（この例ではサーバ名11s、サービスタイプ0x04、Hops数0x01の）ＳＡＰレスポンスとして送信するので、非暗号系クライアント11cからのNearest Service QueryのＳＡＰリクエストに対して常に非暗号系サーバ11sの情報を送信する。暗号系は暗号化装置でHops数５を加算するので、非暗号系より大きくなり除外するので、暗号系／非暗号系端末が混在する同一ネットワーク上で非暗号系通信が可能となる。

【００６８】図２５のネットワークシステムにおいて、暗号系クライアント12cが立ち上がり、暗号系サーバ12sと通信を開始するまでのシーケンスを図２７に示す。図において、暗号系クライアント12cは立ち上がり時にサービスタイプ0x04のNearestService QueryのＳＡＰリクエストを送信し（ステップS21）、暗号化装置2aが受信する（ステップS22）。暗号化装置2aは、端末側送受信部（図２４の21）よりフレームを受信し、フレーム格納メモリ（図２４の22）に格納する。プロトコル判別部（図２４の26）よりNearest Service QueryのＳＡＰフレームと判別され、ＳＡＰ処理部（図２４の28）に渡す。ＳＡＰ処理部において端末からのNearest Service QueryのＳＡＰリクエストに対するサーバ情報テーブル33（図２４の33）に予め設定されているサーバ情報、本

例ではサーバ名12s、サービスタイプ0x04、Hops数02のサーバ情報に基づいてＳＡＰレスポンスフレームを作成し、端末側送受信部よりクライアント12cに送信する（ステップS23）。

【００６９】暗号系クライアント12cはＳＡＰレスポンスフレームを受信し（ステップS24）、ＳＡＰレスポンスフレームに設定されているサーバのネットワーク番号（図５のSP6）に対するＲＩＰリクエストフレームを送信する（ステップS31）。暗号化装置2aは、端末側送受信部（図２４の21）よりフレームを受信し、フレーム格納メモリ（図２４の22）に格納する。プロトコル判別部（図２４の26）よりＲＩＰフレームと判別され、ネットワーク側送受信部よりそのまま送信する（ステップS32）。ルータ4aはＲＩＰリクエストを受信し（ステップS33）、レスポンスを送信する（ステップS34）。

【００７０】暗号化装置2aはネットワーク側送受信部（図２４の23）よりフレームを受信し、フレーム格納メモリ（図２４の22）に格納する。プロトコル判別部（図２４の26）よりＲＩＰフレームと判別され、端末側送受信部よりそのまま送信（ステップS35）し、暗号系クライアント12cが受信する（ステップS36）。ＲＩＰレスポンスに基づき、サーバ12s宛に通信を開始する（ステップS41）。暗号化装置2aは、端末側からフレームを受信するとフレーム格納メモリ（図２４の22）に格納し、プロトコル判別部（図２４の26）に渡す。プロトコル判別部においてデータフレームと判断し、フレームのデータ部（図２のX11）以降を暗号化して送信する（ステップS42）。ルータ4aはルーティングテーブルに従い、宛先アドレス宛にフレームを送信する（ステップS43）。

【００７１】暗号化装置2bはネットワーク側からフレームを受信するとフレーム格納メモリ（図２４の22）に格納し、プロトコル判別部（図２４の26）に渡す。プロトコル判別部においてデータフレームと判断し、フレームのデータ部（図２のX11）を復号して送信し（ステップS44）、暗号系サーバ12sが受信する（ステップS45）。また、暗号系サーバ12sから暗号系クライアント12cへはステップS41からステップS45の逆をたどってデータが送信される。

【００７２】以上のように、クライアントを収容する暗号化装置が暗号系サーバを指定して立ち上げるので、暗号系のサーバと暗号系のクライアントを接続できる。また、図２８に示すようにルータがないシステム構成であっても、クライアント11cからのNearest Service QueryのＳＡＰリクエストに対し、暗号系サーバ12sに接続されている暗号化装置2bがNearest Service QueryのＳＡＰリクエストを廃棄し、非暗号系サーバ11sは自サーバテーブルでHops数最小のサーバ名11sを通知するので、非暗号系サーバと非暗号系クライアントを接続できる。以上のように、暗号系サーバのHops数を大きい値にしておき、非暗号系クライアントを立ち上げるとき、Nearest Service QueryのＳＡＰリクエストを受信したサーバまたはルータはHops数の小さい値を持つサーバを選んで、そのサーバ名を通知し、暗号化装置はネットワークからのNearest Service QueryのＳＡＰリクエストを廃棄するので、暗号系サーバを選ぶことなく、非暗号系サーバと非暗号系クライアントを接続できる。従って、暗号系／非暗号系端末が混在するネットワーク上で暗号と非暗号の通信が可能となる。

【００７３】本実施例ではバス型のＬＡＮ上での適用例を示したが、リング型のＬＡＮ上またはＷＡＮ上でも同様の効果を奏する。また、端末側送受信部にネットワークを接続し、ネットワークへの中継時に暗号化／復号処理を行う場合も同様の効果を奏する。

【図面の簡単な説明】

【図１】　実施の形態１による暗号化装置の構成図である。

【図２】　ＩＰＸフレームのフォーマットである。

【図３】　ＲＩＰリクエストのフレームフォーマットである。

【図４】　ＳＡＰリクエストのフレームフォーマットである。

【図５】　ＳＡＰレスポンスのフレームフォーマットである。

【図６】　暗号化せずに同一ネットワーク上のクライアント／サーバが通信する場合のネットワーク構成図である。

【図７】　サーバが自分のサーバ情報を定期的に送信するシーケンス図である。

【図８】　クライアントが立ち上がる時のシーケンス図である。

【図９】　ルータを介してクライアントとサーバを接続する構成を示す図である。

【図１０】　サーバが自分のサーバ情報を定期的に送信するシーケンス図である。

【図１１】　クライアントが立ち上がる時のシーケンス図である。

【図１２】　実施の形態１による暗号通信システムの構成図である。

【図１３】　実施の形態１による暗号通信システムでサーバが自分のサーバ情報を定期的に送信するシーケンス図である。

【図１４】　実施の形態１による暗号通信システムでクライアントが立ち上がる時のシーケンス図である。

【図１５】　実施の形態１による暗号通信システムで暗号系クライアントが非暗号系サーバからのＳＡＰリクエスト受信したときのシーケンス図である。

【図１６】　実施の形態１による暗号通信システムで非暗号系クライアントが暗号系サーバからのＳＡＰリクエスト受信したときのシーケンス図である。

【図１７】　実施の形態１によるルータを含む暗号通信

システムの構成図である。

【図１８】　実施の形態１によるルータを含む暗号通信システムでクライアントが立ち上がる時のシーケンス図である。

【図１９】　暗号用のサービスタイプを複数用いた場合のルータを含む暗号通信システムの構成図である。

【図２０】　実施の形態２による暗号化装置の構成図である。

【図２１】　実施の形態２によるルータを含む暗号通信システムの構成図である。

【図２２】　実施の形態２による暗号通信システムでサーバが自分のサーバ情報を定期的に送信するシーケンス図である。

【図２３】　実施の形態２による暗号通信システムで暗号系クライアントが新たな非暗号サーバに接続する例を示す図である。

【図２４】　実施の形態３による暗号化装置の構成図である。

【図２５】　実施の形態３による暗号通信システムの構成図である。

【図２６】　実施の形態３による暗号通信システムでサーバが自分のサーバ情報を定期的に送信するシーケンス図である。

【図２７】　実施の形態３による暗号通信システムで暗号系クライアントが立ち上がる時のシーケンス図である。

【図２８】　実施の形態３によるルータがない場合の暗号通信システムの構成図である。

＊【図２９】　従来例による通信ネットワークの構成を示す図である。

【図３０】　従来例のフレームを暗号化する範囲を示す図である。

【符号の説明】

１　端末

２、２ａ、２ｂ、２ｃ、２ｄ　暗号化装置

３、３ａ、３ｂ　ネットワーク

４ａ　ルータ

１１ｃ　暗号化装置が接続されないクライアント

１１ｓ　暗号化装置が接続されないファイルサーバ

１２ｃ　暗号化装置が接続されたクライアント

１２ｓ、１３ｓ　暗号化装置が接続されたファイルサーバ

２１　端末側送受信部

２２　フレーム格納メモリ

２３　ネットワーク側送受信部

２４　ＲＯＭ／ＲＡＭ

２５　中央処理部

２６　プロトコル判別部

２７　データ暗号／復号処理部

２８　ＳＡＰ処理部

３０、３０ａ、　透過処理アドレステーブル

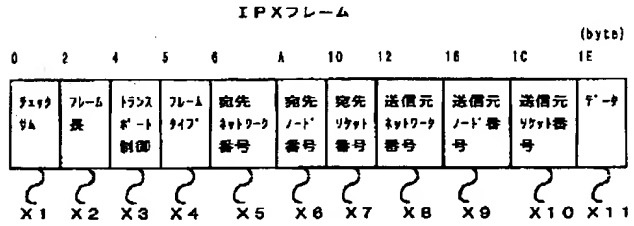
３１、３１ｂ、３１ｃ　透過処理サーバテーブル

３２　Hops数メモリ

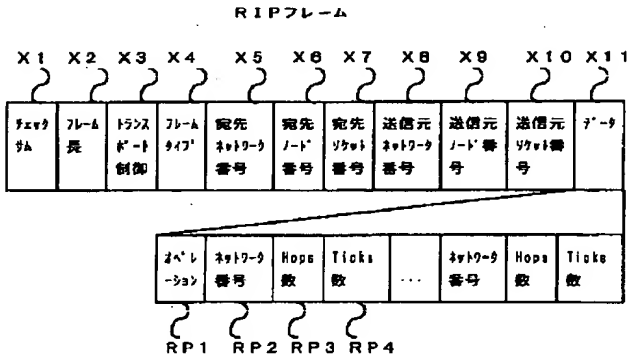
３３　サーバ情報テーブル

５１、５２、５３　サーバテーブル

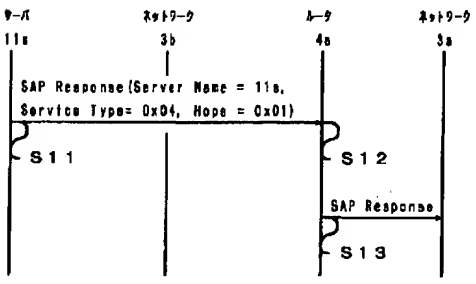
【図２】



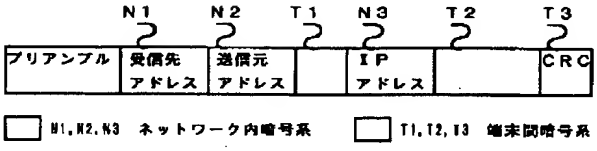
【図３】



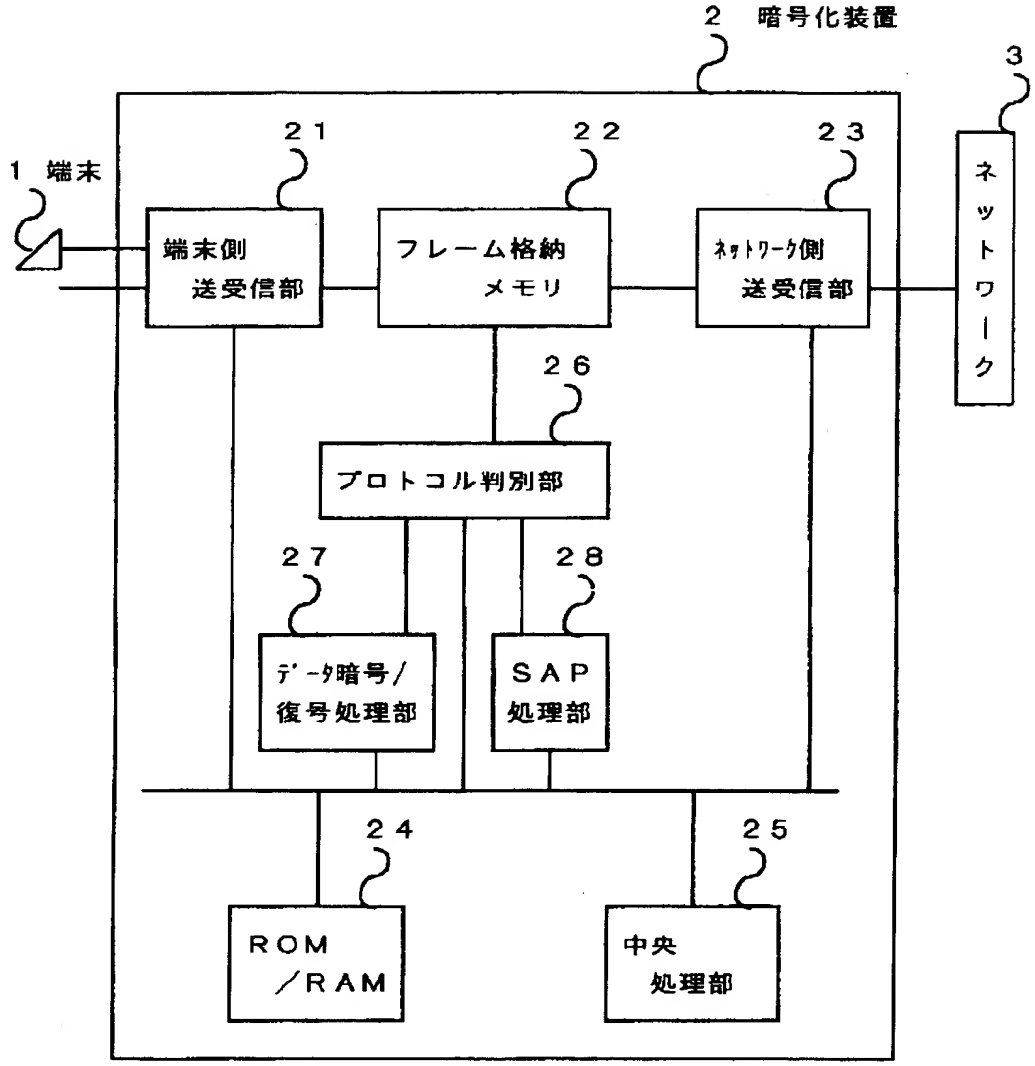
【図１０】



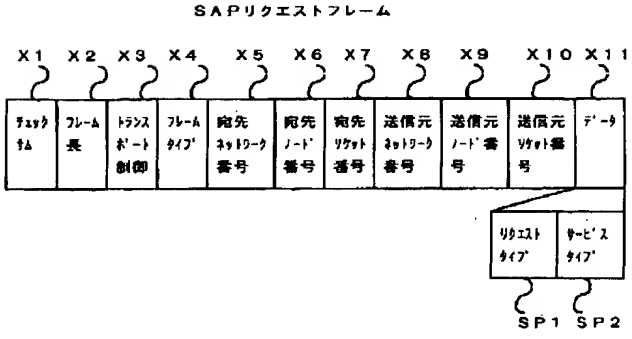
【図３０】



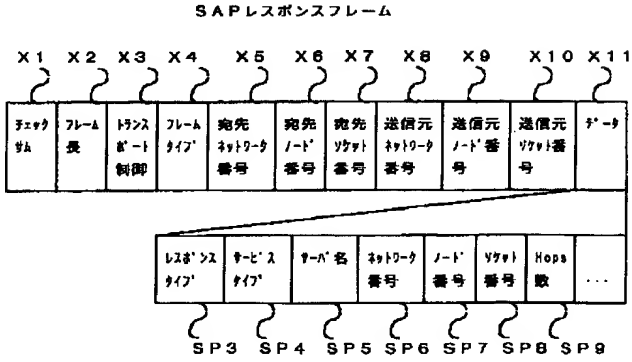
【図１】


2　暗号化装置
3
21
22
23
1　端末
端末側
送受信部
フレーム格納
メモリ
ネットワーク側
送受信部
ネットワーク
26
プロトコル判別部
27
28
データ暗号/
復号処理部
SAP
処理部
24
25
ROM
/RAM
中央
処理部

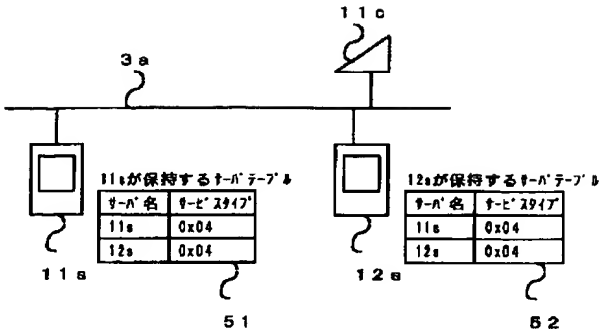
【図４】


SAPリクエストフレーム
X1 X2 X3 X4 X5 X6 X7 X8 X9 X10 X11
チェックサム
フレーム長
トランスポート制御
フレームタイプ
宛先ネットワーク番号
宛先ノード番号
宛先ソケット番号
送信元ネットワーク番号
送信元ノード番号
送信元ソケット番号
データ
リクエストタイプ
サービスタイプ
SP1 SP2

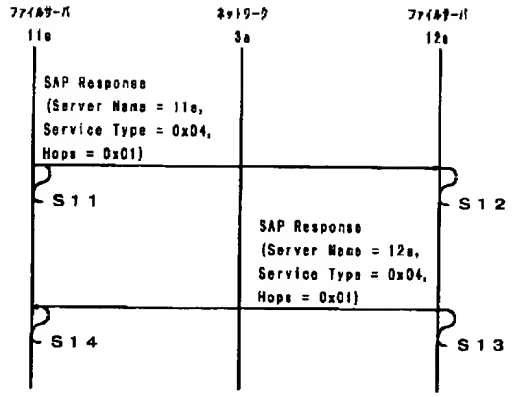
【図５】


SAPレスポンスフレーム
X1 X2 X3 X4 X5 X6 X7 X8 X9 X10 X11
チェックサム
フレーム長
トランスポート制御
フレームタイプ
宛先ネットワーク番号
宛先ノード番号
宛先ソケット番号
送信元ネットワーク番号
送信元ノード番号
送信元ソケット番号
データ
レスポンスタイプ
サービスタイプ
サーバ名
ネットワーク番号
ノード番号
ソケット番号
Hops数
...
SP3 SP4 SP5 SP6 SP7 SP8 SP9

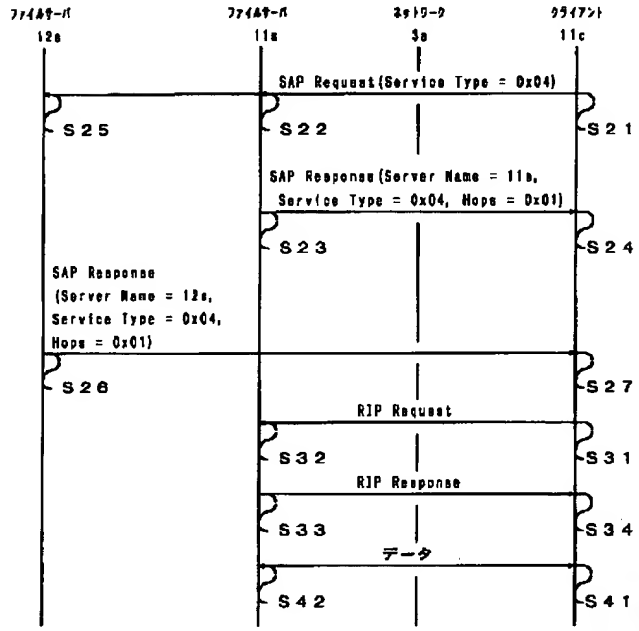
【図６】



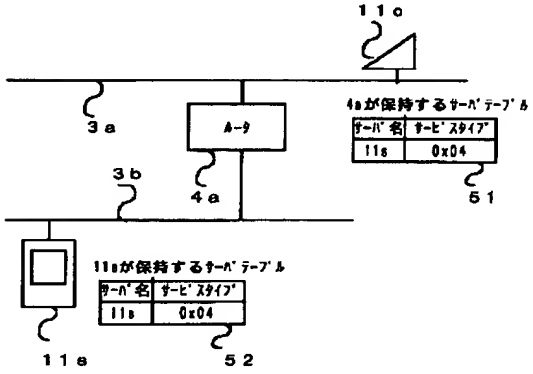
【図７】



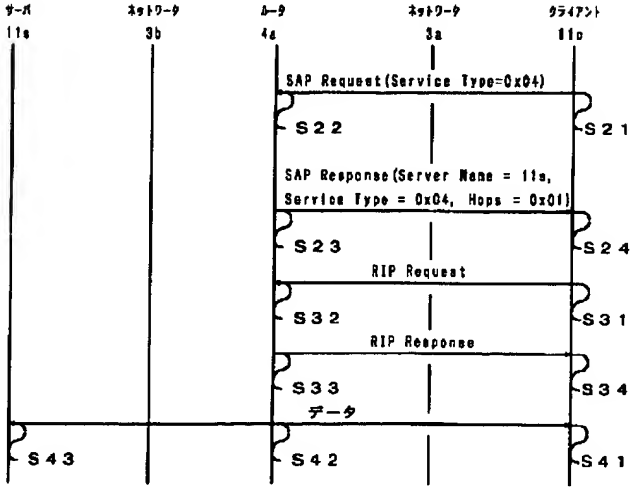
【図８】



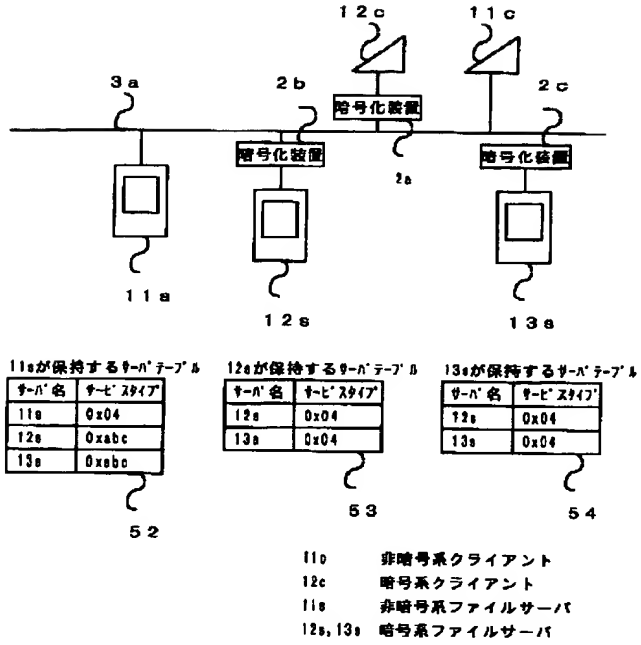
【図９】



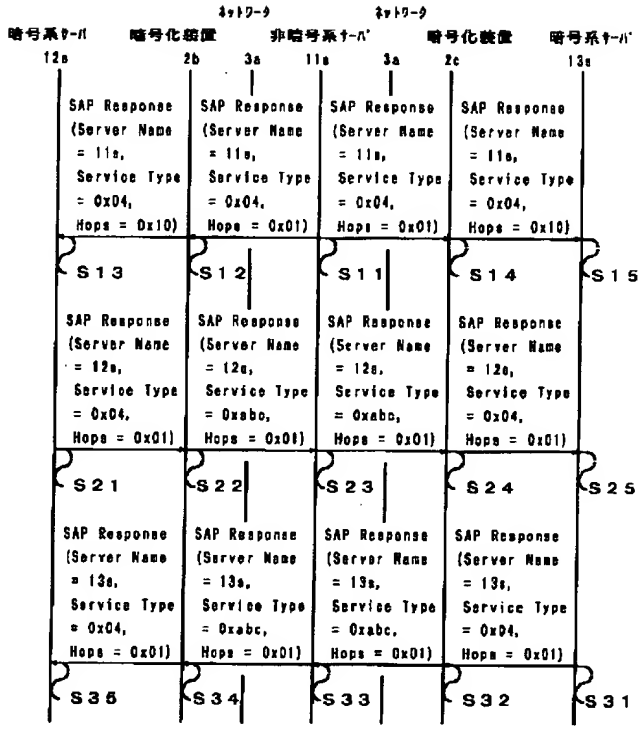
【図１１】



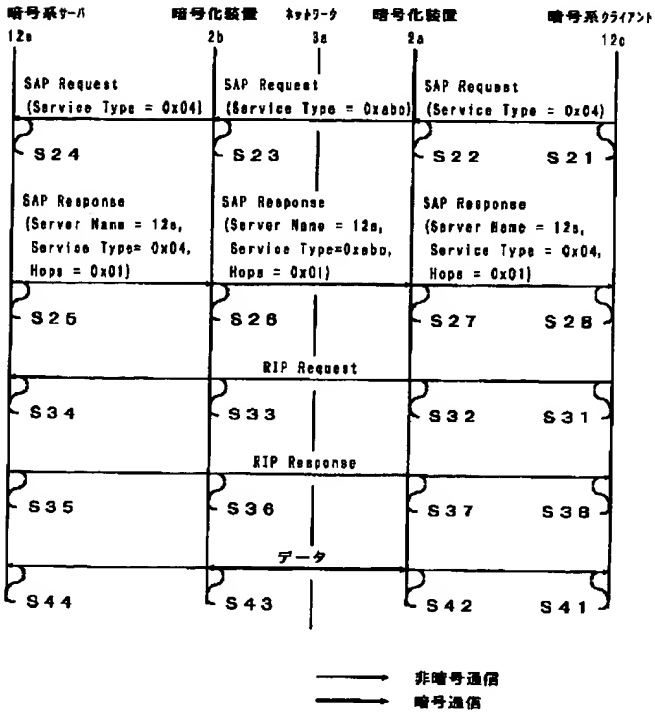
【図１２】



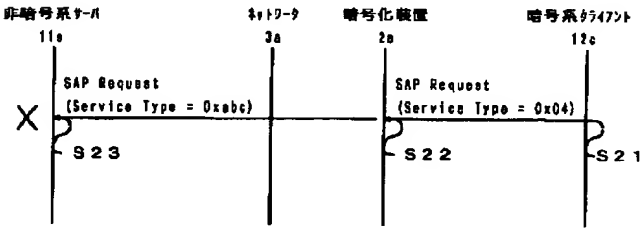
【図１３】



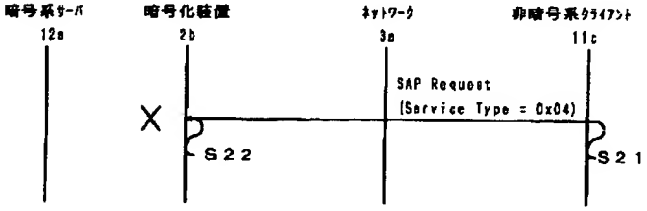
【図１４】



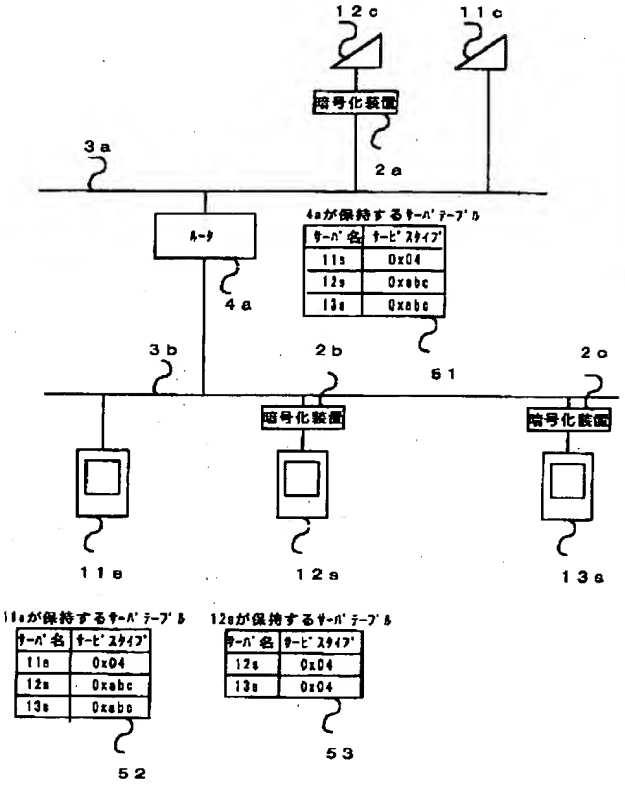
【図１５】



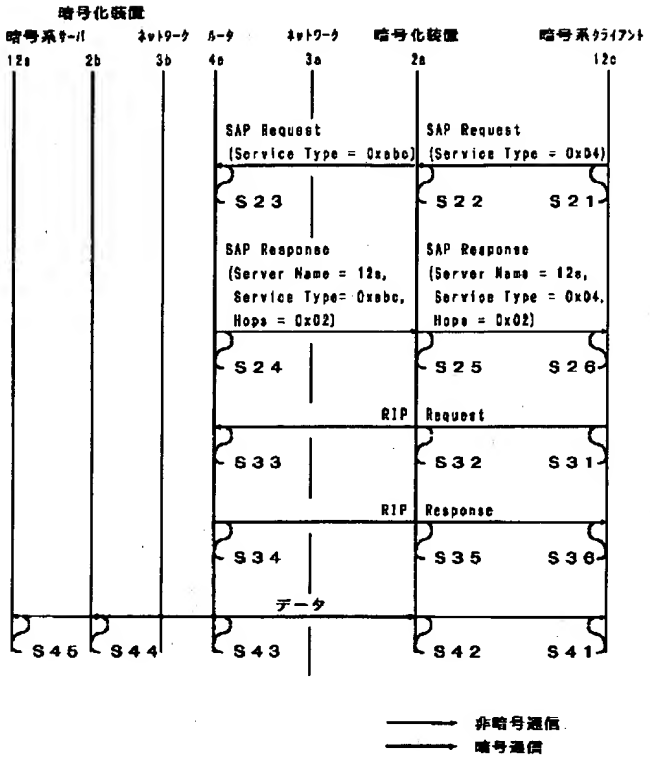
【図１６】



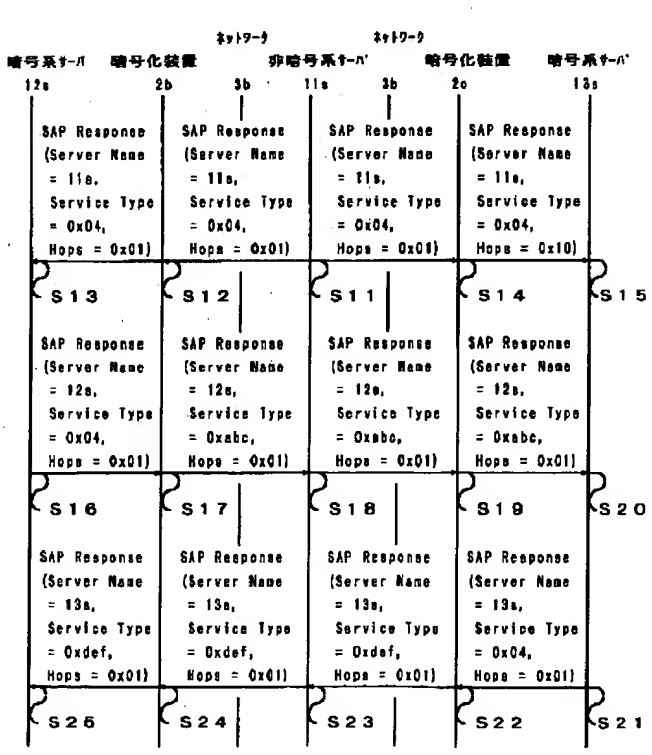
【図１７】



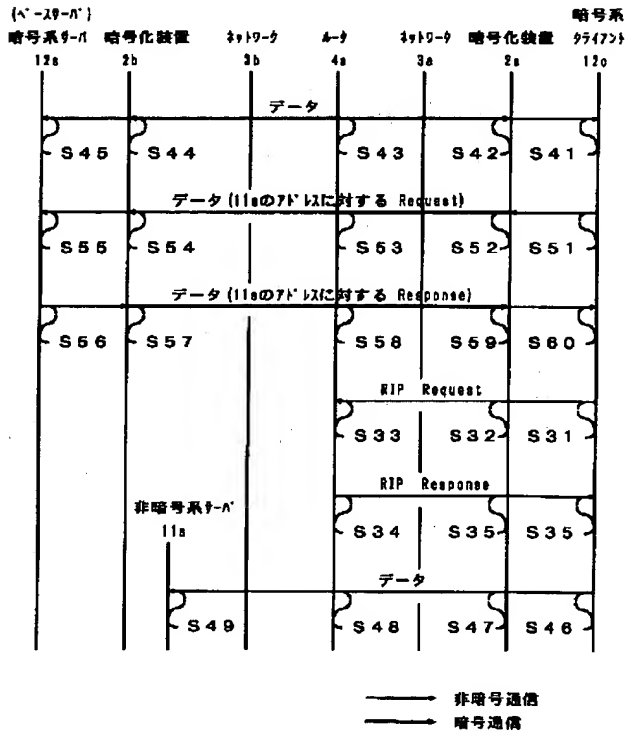
【図１８】



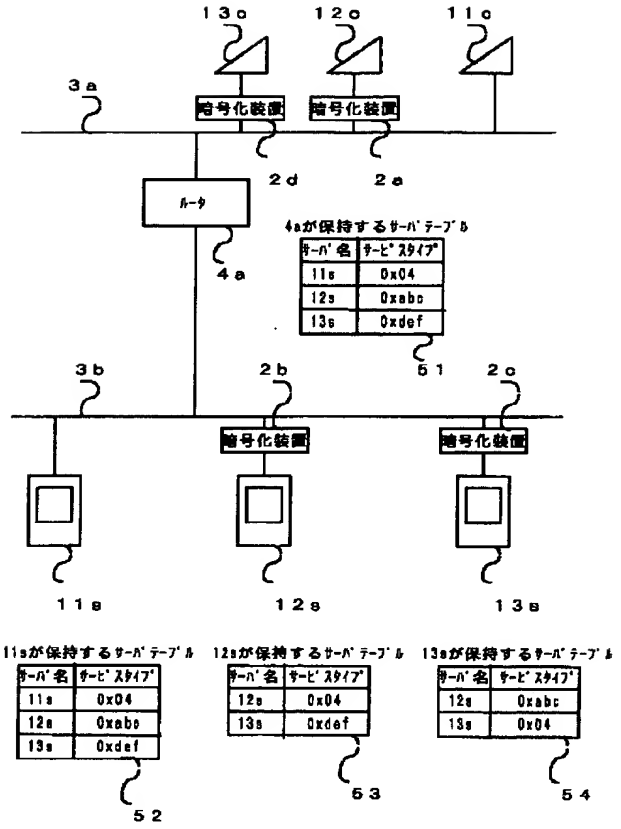
【図２２】



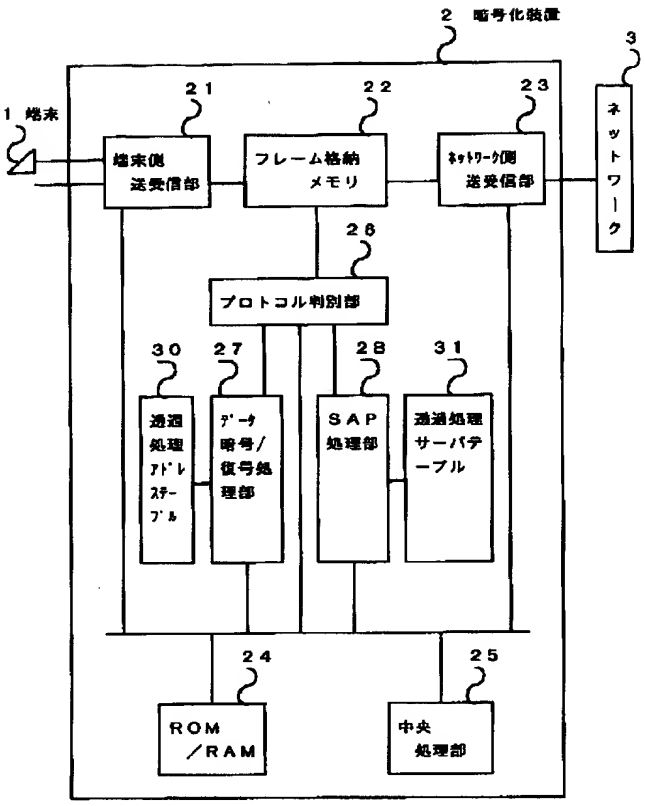
【図２３】



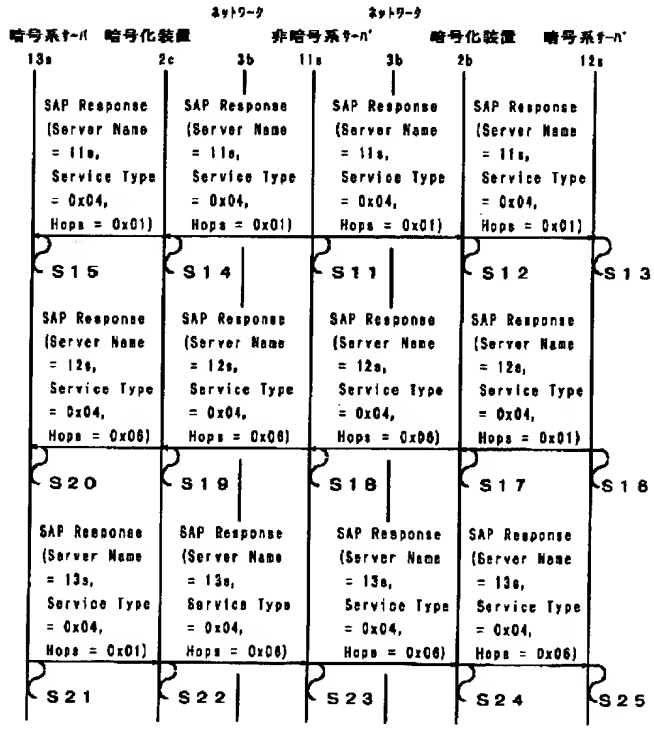
【図１９】



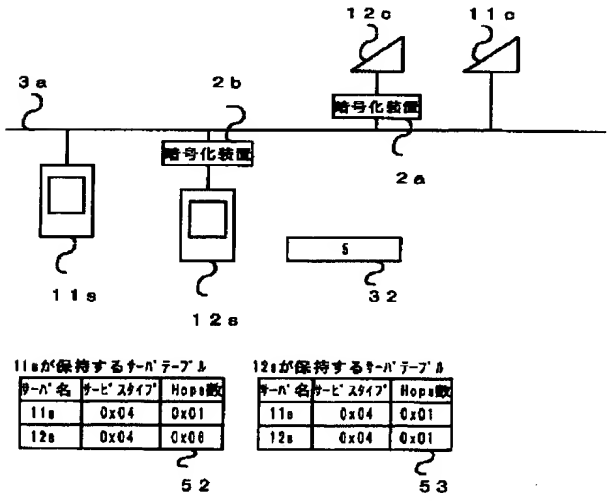
【図２０】



【図２６】

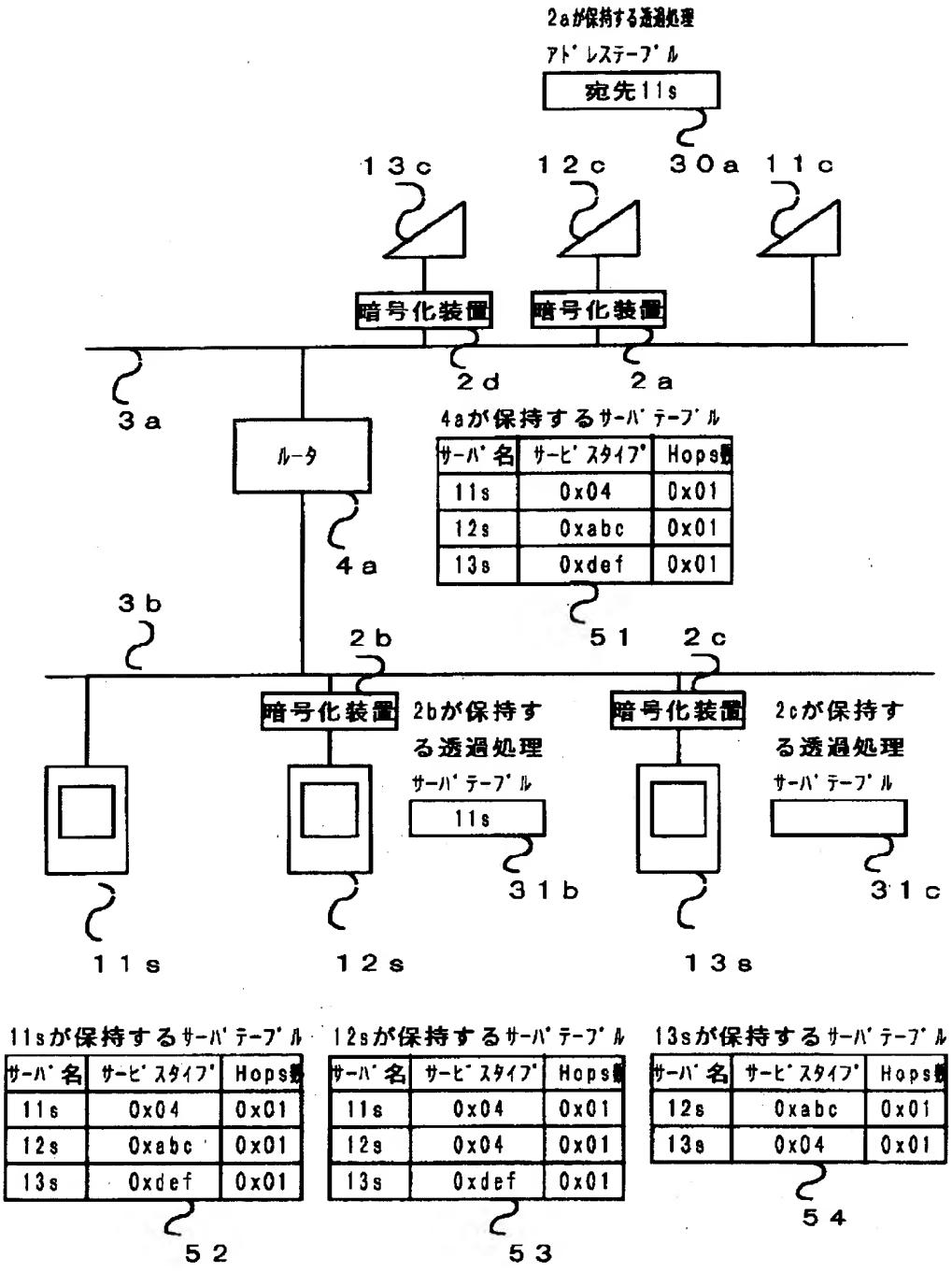


【図２８】

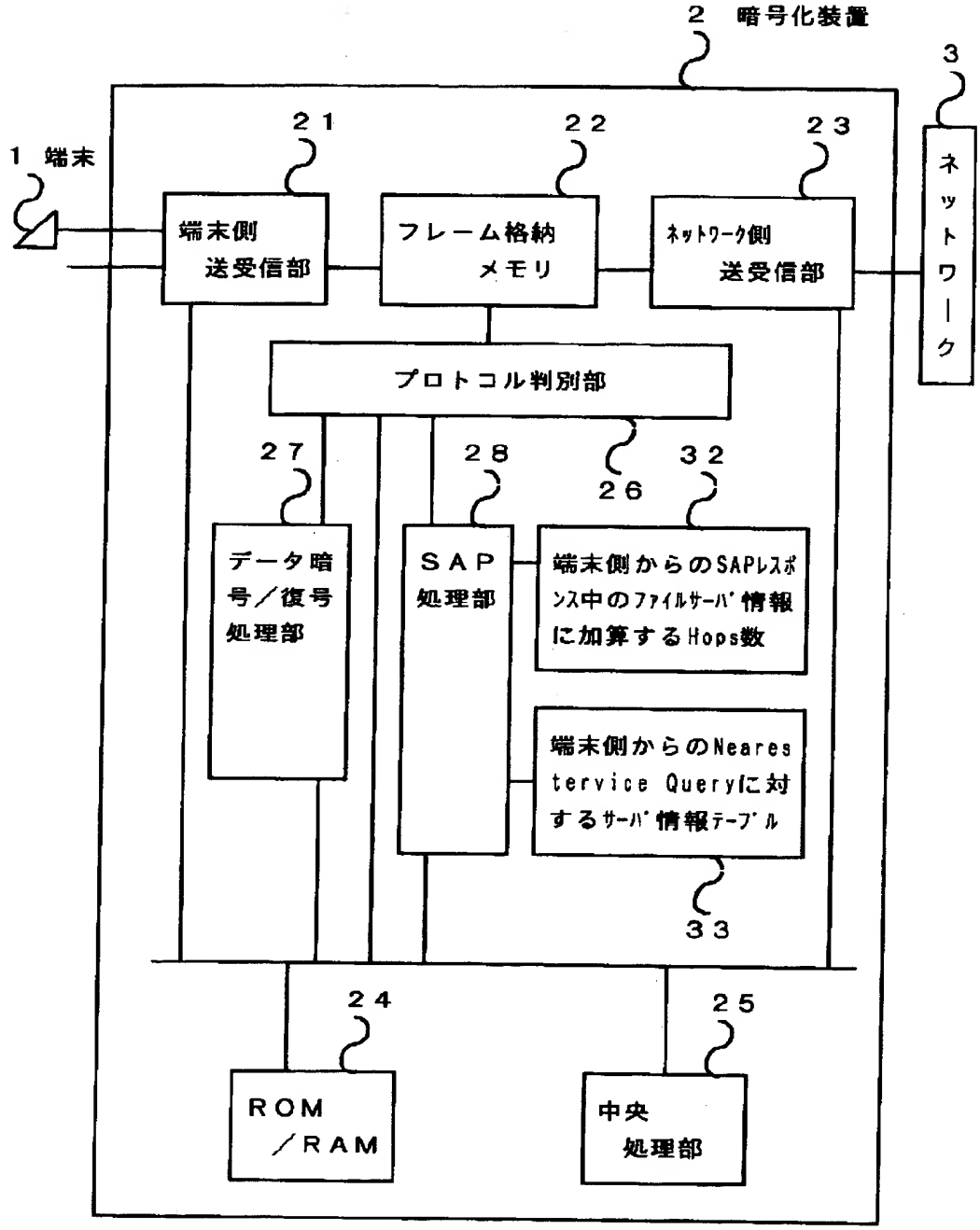


11c　非暗号系クライアント
12c　暗号系クライアント
11s　非暗号系ファイルサーバ
12s, 13s　暗号系ファイルサーバ

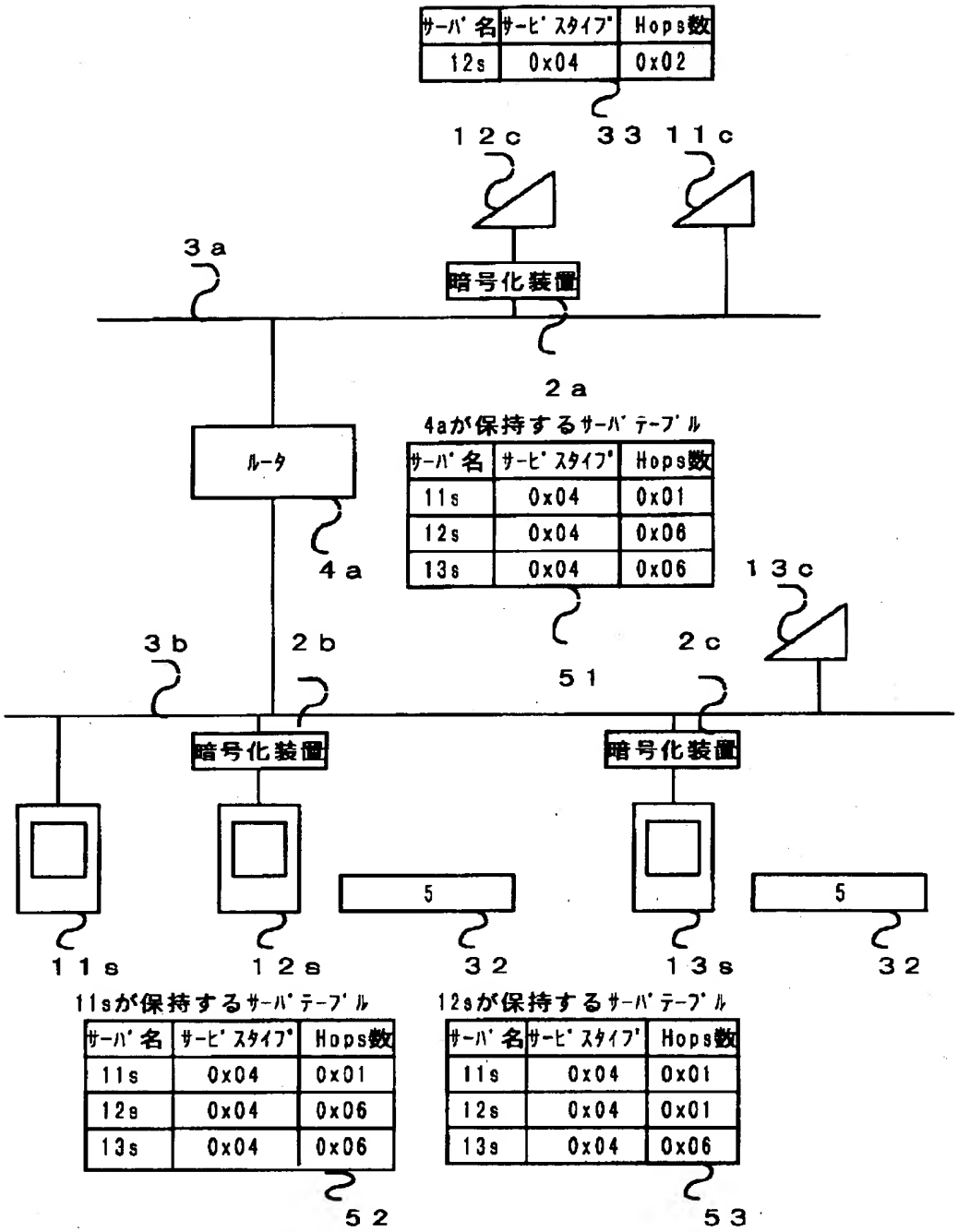
【図２１】


2aが保持する透過処理
ｱﾄﾞﾚｽﾃｰﾌﾞﾙ
宛先11s
30a
13c
12c
11c
暗号化装置
暗号化装置
2d
2a
3a
ルータ
4a
4aが保持するｻｰﾊﾞﾃｰﾌﾞﾙ
ｻｰﾊﾞ名 ｻｰﾋﾞｽﾀｲﾌﾟ Hops数
11s 0x04 0x01
12s 0xabc 0x01
13s 0xdef 0x01
51
3b
2b
2c
暗号化装置
2bが保持する透過処理
ｻｰﾊﾞﾃｰﾌﾞﾙ
11s
31b
暗号化装置
2cが保持する透過処理
ｻｰﾊﾞﾃｰﾌﾞﾙ
31c
11s
12s
13s
11sが保持するｻｰﾊﾞﾃｰﾌﾞﾙ
ｻｰﾊﾞ名 ｻｰﾋﾞｽﾀｲﾌﾟ Hops数
11s 0x04 0x01
12s 0xabc 0x01
13s 0xdef 0x01
52
12sが保持するｻｰﾊﾞﾃｰﾌﾞﾙ
ｻｰﾊﾞ名 ｻｰﾋﾞｽﾀｲﾌﾟ Hops数
11s 0x04 0x01
12s 0x04 0x01
13s 0xdef 0x01
53
13sが保持するｻｰﾊﾞﾃｰﾌﾞﾙ
ｻｰﾊﾞ名 ｻｰﾋﾞｽﾀｲﾌﾟ Hops数
12s 0xabc 0x01
13s 0x04 0x01
54

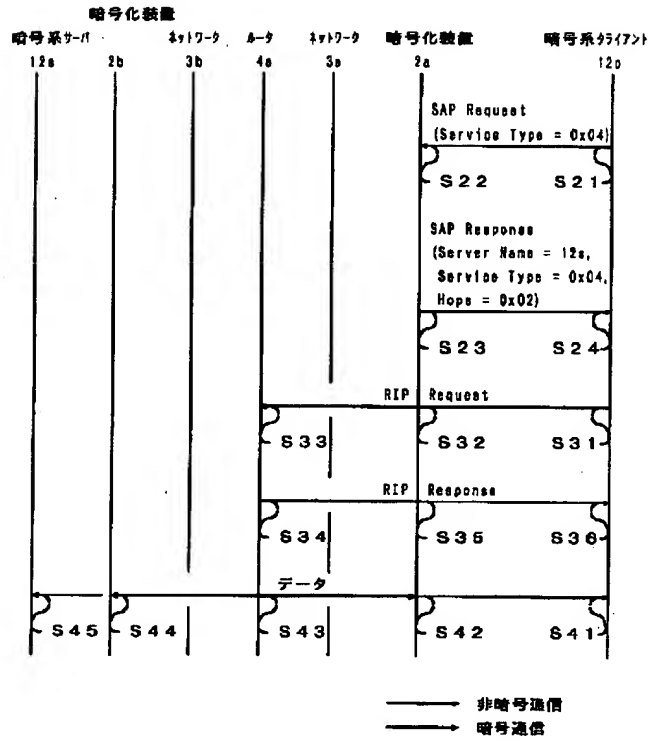
【図２４】


2　暗号化装置
3
ネットワーク
1　端末
21
22
23
端末側
送受信部
フレーム格納
メモリ
ネットワーク側
送受信部
プロトコル判別部
27
28
26
32
データ暗
号／復号
処理部
SAP
処理部
端末側からのSAPレスポンス中のファイルサーバ情報に加算するHops数
端末側からのNearest Service Queryに対するサーバ情報テーブル
33
24
25
ROM
／RAM
中央
処理部

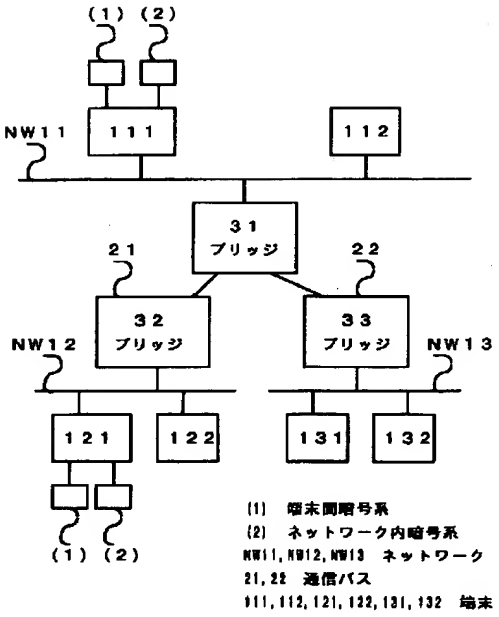
【図２５】


サーバ名 サービスタイプ Hops数
12s 0x04 0x02
33
12c
11c
3a
暗号化装置
2a
4aが保持するサーバテーブル
サーバ名 サービスタイプ Hops数
11s 0x04 0x01
12s 0x04 0x06
13s 0x04 0x06
51
ルータ
4a
13c
3b
2b
2c
暗号化装置
暗号化装置
5
5
11s
12s
32
13s
32
11sが保持するサーバテーブル
サーバ名 サービスタイプ Hops数
11s 0x04 0x01
12s 0x04 0x06
13s 0x04 0x06
52
12sが保持するサーバテーブル
サーバ名 サービスタイプ Hops数
11s 0x04 0x01
12s 0x04 0x01
13s 0x04 0x06
53

【図２７】



【図２９】



フロントページの続き

(72)発明者　厚井　裕司
東京都千代田区丸の内二丁目２番３号　三
菱電機株式会社内